*TNO-rapport*
FEL-99-A142

# Verkenning naar Information Warfare, Information Operations en Information Assurance

TNO Fysisch en Elektronisch Laboratorium

Oude Waalsdorperweg 63
Postbus 96864
2509 JG 's-Gravenhage

Telefoon 070 374 00 00
Fax 070 328 09 61



Datum
juli 1999

Auteur(s)
Ir. H.A.M. Luiijf

| | |
|---|---|
| Opdrachtgever | Ministerie van Defensie |
| Projectbegeleider | LKol. J.J.M.G. Maenen |
| Onderdeel | Defensiestaf/Conceptuele Zaken |
| Rubricering | |
| Vastgesteld door | LKol. J.J.M.G. Maenen |
| Vastgesteld d.d. | 22 juni 1999 |
| Titel | Ongerubriceerd |
| Managementuittreksel | Ongerubriceerd |
| Samenvatting | Ongerubriceerd |
| Rapporttekst | Ongerubriceerd |
| Bijlagen | Ongerubriceerd |
| Exemplaarnr. | 14 |
| Oplage | 57 |
| Aantal pagina's | 90 (incl. bijlagen, excl. RDP & distributielijst) |
| Aantal bijlagen | 2 |



TNO Fysisch en Elektronisch Laboratorium is onderdeel van TNO Defensieonderzoek waartoe verder behoren:

TNO Prins Maurits Laboratorium
TNO Technische Menskunde

Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek TNO

# Managementuittreksel

| | | |
|---|---|---|
| Titel | : | Verkenning naar Information Warfare, Information Operations en Information Assurance |
| Auteur(s) | : | Ir. H.A.M. Luiijf |
| Datum | : | juli 1999 |
| Opdrachtnr. | : | A99D603 |
| IWP-nr. | : | 6128 |
| Rapportnr. | : | FEL-99-A142 |

De veranderingen op het gebied van de Informatie en Communicatie-Technologie (ICT) bieden de krijgsmacht steeds meer mogelijkheden. De moderne krijgsmacht wordt gekenmerkt door een steeds nauwere koppeling van civiele en militaire besturingssystemen en informatie-infrastructuren, ook internationaal. Defensie is daarbij meer en meer afhankelijk geraakt van ICT die in steeds mindere mate door de overheid wordt gecontroleerd. Daarom leidt de toepassing van ICT niet alleen tot nieuwe mogelijkheden, maar ook tot nieuwe kwetsbaarheden.
Dat informatie een lucratief doel en wapen is, is niet nieuw. Toch hebben de ICT-ontwikkelingen geleid tot een groeiend besef dat Information Operations (Info Ops) niet langer fictie zijn en dat gewerkt moet worden aan bescherming van de Nederlandse Krijgsmacht en de Nederlandse samenleving.

Naast Defensie wordt ook door de ministeries van Verkeer en Waterstaat, Economische Zaken en Binnenlandse Zaken en Koninkrijksrelaties in enige mate aandacht besteed aan de problematiek van de kwetsbare Nederlandse en internationale samenleving. Daarbij is nog lang geen sprake van een integrale overheidsbenadering.

Dit rapport bevat de verslaglegging van het verkennend onderzoek dat TNO-FEL uitgevoerd heeft in de periode 1996 tot medio 1999. Het doel was het in kaart brengen van de historische en conceptuele militaire ontwikkeling van Information Warfare, Information Operations en Information Assurance. Andere onderzochte aspecten zijn: de kwetsbare (informatie)infrastructuren en de nationale en internationale ontwikkelingen.

Deze verkenning ligt mede ten grondslag aan de verdere ontwikkeling van het TNO-brede Info Ops en Information Assurance onderzoek en is gebruikt als referentiemateriaal in de Duits-Nederlandse studie Information Operations (opdrachtgever Defensiestaf/afd. Conceptuele Zaken).

# Samenvatting

Het fenomeen "Information Warfare (IW)" en de daaraan gekoppelde begrippen Information Operations (Info Ops) en Information Assurance (IA), is in de afgelopen 3 jaar internationaal gezien in een stroomversnelling terechtgekomen. Het onderwerp staat inmiddels hoog op de militaire agenda's van veel landen. Ook staat het inmiddels op de agenda van veel civiele overheden in veel landen, mede gestimuleerd door de millenniumproblematiek. Overheden, defensies en civiele organisaties zijn in de voorbereiding daarop nadrukkelijk gewezen op de kwetsbaarheden van informatievoorziening en infrastructuren alsmede op de keten-problematiek.

De Nederlandse samenleving bevindt zich op de rand van een echte informatie-revolutie. Informatie is inmiddels al een cruciale productiefactor van betekenis geworden. Het sterk toenemende gebruik van informatie en communicatie-technologie (ICT) schept gelijktijdig nieuwe mogelijkheden maar ook nieuwe kwetsbaarheden. Dit zowel op het gebied van defensiesystemen en -infrastructuren, als op het gebied van civiele systemen en op het overlappende gebied van deze twee domeinen. Voor de vrijheid van handelen van het politiek-militaire beslissingsniveaus is het cruciaal dat door de gebruikers van de systemen en infrastructuren op de juistheid, effectiviteit en tijdigheid van informatie en de ongestoorde werking van de informatievoorziening vertrouwd kan worden.
De dreiging in de "Cyberspace" is aanzienlijk. Bijna dagelijks verschijnen er persberichten, die de kwetsbaarheid van onze informatieinfrastructuren aantonen. Deze worden echter veelal als eenmalig "incident" terzijde geschoven zonder de achterliggende kwetsbaarheid te onderkennen. Het gevaar van dit niet onderkennen kan leiden tot een misplaatst gevoel van onaantastbaarheid.

Tussen medio 1996 en eind 1998 heeft TNO-FEL een achtergrondverkenning uitgevoerd naar het fenomeen "Information Warfare". De bevindingen van deze achtergrondverkenning zijn neergelegd in het interne TNO rapport FEL-98-I268. Door de Nederlandse en Duitse defensies, ondersteund door KMA, TNO en het IABG, wordt momenteel gewerkt aan een gezamenlijke conceptuele studie Information Operations, welke medio 1999 in een bilateraal eindrapport aan de wederzijdse Chefs van Staven gepresenteerd zal worden. Voor het meest actuele Nederlandse inzicht wat betreft Info Ops wordt u verwezen naar dat rapport. Tijdens deze bilaterale NL-DU studie is door TNO echter voortgebouwd op de kennis opgedaan tijdens de eerder genoemde achtergrondverkenning. Het leek dan ook wenselijk om een *externe* versie van het interne TNO-rapport uit te brengen.

Dit rapport behandelt achtereenvolgens de historische ontwikkeling van Information Warfare en aanverwante terminologie en aspecten. Het rapport gaat vervolgens in op het scala aan definities voor Information Warfare en Info Ops. Inmiddels komen deze definities door voortschrijdend inzicht steeds meer naar elkaar toe.

Ook de civiele veiligheid vergt nadrukkelijk aandacht. Om die reden is door TNO een definitie opgesteld voor de term "Information Assurance", welke de civiele defensieve Info Ops aspecten afdekt.

Bovendien brengt deze verkenning de Info Ops en Information Assurance/ Critical Infrastructure Protection ontwikkelingen in andere landen in beeld[1] voor zover deze ons bekend zijn en wordt ingegaan op de vraag: wat is er nieuw? Ook wordt aangegeven welke ambitie TNO op dit gebied heeft.

---

1 Dit rapport bevat enkele actualisaties ten opzichte van het eerder genoemde interne FEL-rapport.

# Inhoud

# 1. Inleiding

## 1.1 Kwetsbaarheid informatie-infrastructuren

> "The reason why the enlighted ruler and the wise general are able to conquer the enemy whenever they lead the army and can achieve victories that surpass those of others is because of foreknowledge"
>
> uit: The art of War. Sun Tzu

De mensheid is afhankelijk geworden van technologie in het dagelijks leven, in het werk, bij reizen, voor communicatie, voor ontspanning en ook bij het bereiden van een maaltijd in de magnetron. De samenleving en de politieke vorm daarvan, de staat, is daarbij gaan leunen op technologie en de onderling verbonden technische systemen voor verkeersbegeleiding, financiële handelingen, energiedistributie, controle op uitkeringen volgens de sociale wetgeving, communicatie-infrastructuren, onderwijs, hulpdiensten, crisismanagement, diplomatie en vrede stichten.

In het verleden betrof dit sterk door de Staat gereguleerde, separate systemen. Inmiddels zijn veel van deze systemen nauw met elkaar, soms over enkele Staten heen of zelfs mondiaal, verweven. Hierbij zijn vele functies verschoven van overheid naar op afstand van de overheid geplaatste, commercieel concurrerende ondernemingen. Door de afhankelijkheid van de samenleving in het informatie-tijdperk van goed werkende (informatie)infrastructuren en sterk vervlochten, diffuse infrastructuren is de kwetsbaarheid van de samenleving aanzienlijk toegenomen.
Het risico is dan ook groot dat dergelijke kwetsbaarheden uitgebuit worden door activisten, terroristen en zelfs staten - al dan niet in oorlog- of crisissituaties -, daarbij gebruik makend van *nieuwe doctrines*. Het voordeel (soms ook nadeel) van de informatiemaatschappij voor een aanvaller is dat aanvallen *geen nabijheid in tijd en plaats* (en daarmee kwetsbaarheid) meer vereisen, wat een nadeel is voor de bedreigde dan wel aangevallen partij. Een simpele PC kan geheel autonoom een programma starten waarmee aan de andere kant van de wereld kwetsbaarheden in de informatie-infrastructuur uitgebuit worden. Het aan te vallen systeem of infrastructuur kan daarbij zowel militair als civiel van aard zijn. Ook is een combinatie mogelijk indien defensie gebruik maakt van civiele informatie of infra-structuren die aangevallen worden.

Informatie en informatie-infrastructuren dienen dan ook net als andere eigendommen als landsbelang beschermd te worden. De bescherming betreft zowel het intellectuele eigendom als de bescherming tegen ongeoorloofde 'afname' en 'interventie'.

Gezien deze ontwikkeling is enkele jaren geleden binnen de Amerikaanse defensie dan ook de term "Information Warfare" geïntroduceerd. Men realiseerde zich, dat enerzijds de afhankelijkheid van informatie-infrastructuren het militaire apparaat steeds kwetsbaarder maakt voor verstoringen. Anderzijds levert een snellere en betere informatievoorziening een voorsprong op ten opzichte van tegenstanders. Niets nieuws omdat dat al eeuwenlang tactiek is voor overheden, militaire strategen, bedrijven en zelfs individuele personen.
Offensief gezien kan het uitschakelen van de informatie-infrastructuur van een tegenstander dan wel het introduceren van onjuiste informatie in zijn informatie--infrastructuur tot verlamming van de tegenstander leiden.

Information Operations (Info Ops) is het voor eigen doeleinden aanvallen van informatie en infrastructuren van de tegenstander (offensief), het gebruik van eigen informatie(bronnen) voor het adequaat en efficiënt uitvoeren de eigen processen (effectief gebruik) en de bescherming van de eigen informatie en infrastructuren tegen verstoring en aanvallen (defensief; bescherming). Information Assurance is de bescherming van de eigen "assets" tegen interne onveiligheid en externe dreigingen.

De hierboven genoemde omschrijvingen zijn losse beschrijvingen van de preciezere definities die zijn opgenomen in hoofdstuk 3.

Parallel aan de militaire wereld ontdekken steeds meer overheden, utiliteits-bedrijven en ook grote commerciële ondernemingen dat ook de kwetsbaarheid van hun (informatie)infrastructuur enorm is toegenomen.

*Voor overheden is duidelijk geworden, dat zij hun klassieke taak van de bescherming van het eigen land niet meer goed kunnen uitvoeren. Dit omdat de kennis en zeggenschap over kritische informatie-infrastructuren grotendeels buiten de overheid is komen te liggen.*

Men is voor een groot deel afhankelijk geworden van commerciële en inmiddels niet meer onder directe overheidsinvloed staande infrastructuren (bijv. telefonie-netwerken, datanetwerken, GSM/mobiel, elektriciteitsbedrijven).
Dusdanig zelfs, dat het de vraag is of grotere incidenten in de informatie--infrastructuur niet zullen leiden tot een onbeheersbare kettingreactie en het ineenstorten van die infrastructuur en daarmee van een deel van de samenleving. Met name komt daarmee de bescherming van de, in ons geval de Nederlandse, samenleving in het geding. Hierbij moet ruim gekeken worden. De Nederlandse samenleving is door de wereldwijde integratie van informatie-infrastructuren ook kwetsbaar voor verstoring buiten de landsgrenzen. Denk hierbij ook aan de allianties, bondgenootschappen en ook internationale financiële en economische supranationale verbanden.

De beschermer van de samenleving, de overheid, dient dan ook rekening te houden met andere concepten van oorlogvoering, zoals 'Informatie- en Communicatie-

technologie als aanvalswapen'. Hierbij dienen traditionele defensie paradigma's bij verdediging als 'fysiek of visueel contact', 'weten wie de aanvaller is' en 'schaalgrootte gerelateerd aan aanvalssterkte' opnieuw bezien te worden.

In dit rapport wordt ingegaan op deze ontwikkelingen en op de problematiek voor de Nederlandse defensie en de Nederlandse overheid als geheel. De vraag daarbij is hoe de belangen van de Nederlandse Staat en "BV Nederland" veiliggesteld kunnen worden tegen kwetsbaarheden en dreigingen die onder de noemers "(Defensieve) Information Warfare", "Information Operations" en "Information Assurance" geplaatst kunnen worden.

## 1.2 Het verkennend onderzoek

De verkenning had als oorspronkelijk doel inzicht te verschaffen in de volgende vragen:

- Wat is Information Warfare (IW) en wat omvat dit ?
- Wat is er nieuw of is het oude wijn in nieuwe zakken? Welke relatie ligt er met bestaande onderzoeksgebieden en technologieën?
- Wat is de werkelijkheid en de fictie van Information Warfare?
- Wat is Defensieve Information Warfare (IW-D) en Information Operations (Info Ops)?
- Welke zijn de IW-onderzoeksterreinen waar TNO actief moet zijn, mede gezien in het licht van de werkzaamheden waarmee en werkterreinen waarop TNO reeds actief is. Wat kan TNO op dit terrein betekenen? [2]

Gedurende de looptijd van de verkenning zijn enkele aanvullende doelen gesteld. Hieronder het verzorgen van lezingen en publicaties [Luiijf98, Luiijf99a, 99b] en het becommentariëren van concepten van NATO documenten op dit gebied.

## 1.3 Werkwijze, publicaties

Binnen de TNO-FEL groep Beveiliging is van begin 1996 tot begin 1997 in eerste instantie een literatuurstudie uitgevoerd. Dit naar aanleiding van deelname in mei 1996 door een medewerker aan de "InfoWarCon 96" conferentie te Brussel. Begin juni 1997 is door twee FEL-medewerkers deelgenomen aan een overzichtscursus "Information Warfare" gegeven door Edward Waltz en georganiseerd door H.Silver and Associates.

Medio november 1997 heeft Luiijf op uitnodiging als gastspreker deelgenomen aan de door H.Silver and Associates georganiseerde conferentie "Information Warfare". Voorafgaand aan deze conferentie is aan de FEL-website een "

---

2 Deze aspecten komen alleen in het interne TNO rapport aan de orde.

Information Warfare and Information Defense URLography" hoofdpagina toegevoegd (*http://www.tno.nl/instit/fel/infoops*). Deze pagina verwijst naar een aantal webbronnen onderverdeeld naar een aantal IW-deelonderwerpen.

Tijdens laatstgenoemde conferentie kwam het contact op Info Ops gebied tot stand tussen TNO en de KMA. Hieruit volgde een uitnodiging voor een discussie-bijeenkomst op het IDL met medewerkers van Defensiestaf en Krijgsmachtdelen die dit onderwerp met grote belangstelling volgden.

Op basis van al deze informatiebronnen, literatuur en verkenningen is begin 1998 een eerste intern conceptrapport opgesteld. Die versie is voorgelegd aan de meest direct betrokken TNO-FEL groepen om te komen tot een eerste interne afstemming.
Vrijwel gelijktijdig ontwikkelde binnen NATO zich consensus op het brede terrein van Information Warfare, Information Operations en Information Assurance.

In de loop van 1998 en begin 1999 zijn door TNO verschillende externe presentaties gegeven over het onderwerp Information Warfare, Information Operations en Information Assurance: AOC (tezamen met Bgen. Prof. J.M.J. Bosch), Club de Berne (gastheer MinBZK/BVD; [Luiijf98]), gastcollege op de KMA (op uitnodiging van en tezamen met Bgen. Prof. J.M.J. Bosch), Leergang Top-Management Defensie LTD98-2 en 99-1, EICAR'99 conferentie, KIVI afd. Defensieonderzoek, T.U. Eindhoven/EUForce. Dit naast een aantal presentaties voor externe bezoekers van het FEL.

Van 8 tot en met 11 september 1998 werd door 2 FEL medewerkers deelgenomen aan de achtste InfoWar conferentie (InfowarCon'98 te Washington [InfoW98]. Daar zijn geen grote witte vlekken in de reeds aanwezige perceptie van Info Ops en critical infrastructure protection naar voren gekomen. Hierna is het interne TNO-rapport als weerslag van een langlopende verkenning eind 1998 uitgebracht.

## 1.4 Rapportindeling

In dit rapport wordt een overzicht gegeven van het fenomeen Information Warfare (IW) in brede zin. Aangegeven wordt wat Information Warfare, Information Operations en Information Assurance is en op welke deelgebieden TNO geëquipeerd is.

Hoofdstuk 2 gaat in op de historische ontwikkeling van Information Warfare en behandelt welke "scholen" er zijn en gaat deels in op de vraag "wat is er nieuw"? De relatie wordt gelegd met het Nolan-model, waarbij aangegeven wordt dat we momenteel in de beginfase zitten van de "Information Warfare" ontwikkeling.

Voor ons eigen houvast is in 1998 aansluiting gezocht bij de zich ontwikkelende NATO-definitie van Information Operations, welke sinds 1998 ook door Defensie als leidend wordt beschouwd. Daarnaast is door ons een Nederlandse definitie voor Information Assurance opgesteld, die met name ook het civiele domein omvat. Deze definities worden behandeld in hoofdstuk 3. Bijlage B bevat een aantal definities zoals die door andere landen gehanteerd worden.

In hoofdstuk 4 worden de verschillende modellen gepresenteerd die de verschillende aspecten van Information Warfare, Information Operations, Command & Control Warfare en Information Assurance alsmede hun onderlinge relaties weergeven.

In hoofdstuk 5 wordt de ons laatst bekende internationale militaire en civiele ontwikkelingen m.b.t. Information Operations, Information Assurance en infrastructuurbescherming op een rij gezet.

Hoofdstuk 6 behandelt het onderwerp "wat is er nieuw". Het volgende hoofdstuk positioneert TNO.

Naast een lijst met literatuur- en webverwijzingen (hoofdstuk 8) en de trefwoord-index, bevatten de bijlagen een uitgebreide lijst van relevante afkortingen (bijlage A) en een aantal, deels historische, IW, C2W en Info Ops definities (bijlage B).

# 2. Eerste verkenning van de Information Warfare omgeving

Dit hoofdstuk verkent eerst de grenzen van het begrip Information Warfare. Dit als voorbereiding op het volgende hoofdstuk waar ingegaan wordt op de definitie van de termen rondom het begrip Information Warfare (IW).

## 2.1 De historie en grondleggers

Voor het begrip Information Warfare is geen eenduidige oorsprong aan te wijzen. Terugkijkend zijn er een aantal studies en artikelen aan te wijzen, die mede bijgedragen hebben tot de opkomst van het begrip Information Warfare. Daarnaast is de Golfoorlog en de analyses daarvan de aanjager geweest in de discussies over Information Warfare.

Tot de lijst van belangrijke *historische* Information Warfare publicaties behoren:

- Alvin and Heidi Toffler, 1993, "War and Anti-war: Survival at the Dawn of the 21st Century" [Toffler].
- Alan Campen in AFCEA 1992, "The First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War".
- Jon Arquilla en David Ronfelt, 1993, "Cyberwar is coming" waarin voor het eerst de termen CyberWar en Netwar geïntroduceerd zijn [Arquil].
- Winn Schwartau, 1994, "Chaos on the Electronic Superhighway": met de verwevenheid van miljoenen systemen en netwerken kunnen we een elektronisch Pearl Harbor tegemoet zien. [WSchw]
- Martin Libicki, 1995: "What is Information Warfare?".
- Stuart Johnson and Martin Libicki, 1995: "Dominant battlespace knowledge".

In de volgende paragrafen worden de in deze publicaties aangegeven ideeën en IW-type indelingen nader belicht.

De basis voor de IW-ontwikkeling volgt volgens Alvin en Heidi Toffler uit een essentiële verschuiving die in de maatschappij plaats heeft, de "Third Wave", of wel de informatierevolutie. Volgens hen verschuift het economisch belang, dat enkele honderden jaren nog in de landbouw en het grondbezit lag, via de industriële revolutie naar "Informatie". De belangrijkste aspecten van deze verschuivingen, welke ook op oorlogsvoering en conflicten geprojecteerd worden, worden in Tabel 2.1 genoemd. Al kunnen er kritische kanttekeningen gezet worden bij deze simpele gedachtenvorming, toch hebben de ideeën van de Tofflers de ontwikkeling van de IW-gedachten enorm gestimuleerd.

*Tabel 2.1: Alvin en Heidi Toffler "Third Wave" en "War and Anti-War"*

| Tijdperken | Landbouw-tijdperk | Industrieel tijdperk (vanaf +/- 1750) | Informatietijdperk (ongeveer nu) |
|---|---|---|---|
| **Economiedrijver** | • Landbouw | • Massaproductie | • Specifieke, klantgerichte informatieproductie |
| **Productiemiddel** | • Grond | • Grondstoffen<br>• Kapitaal | • Informatie |
| **Mijlpalen** | • Gewasbeheersing<br>• Irrigatie<br>• Planning<br>• Voedselopslag | • Industriële revolutie (1800) - gereedschappen<br>• Mechanisatie (1850)<br>• Werkanalyse (1900)<br>• Statistische controle (1945)<br>• Numeriek bestuurd (1976)<br>• Computer bestuurd (1987) | • Computer (1943)<br>• Microprocessor (1975)<br>• Databases (1975+)<br>• Kennisextractie uit gegevens (1985+)<br>• ARPAnet (1980) |
| **Ontstaan van conflicten** | • Conflict tussen land-eigenaren<br>• Conflict tussen heersers | • Regionale en geo-economische strijd<br>• Conflict tussen legers van landen | • Geo-informatiestrijd<br>• Conflict tussen ideologieën en economieën |
| **Basisprincipes van oorlogsvoering** | • Uitputtingsoorlog van infanterie of marine | • Massavernietiging<br>• Uitputtingsoorlog van machines<br>• Bewapening | • Uitputting van slagkracht en mogelijkheden<br>• Volledig controle over perceptie van tegenpartij<br>• Complex en adaptief |

## 2.2 Hoofdstromen of Information Warfare-"scholen"

Binnen de grote verscheidenheid aan Information Warfare publicaties zijn ruwweg een drietal hoofdstromen te onderkennen;

- *Third wave approach* door Alvin Toffler [Toffler] en zijn "school": een zeer futuristische, bijna new age-achtige, benadering. Deze omvat het scala van "wij zijn nu reeds in oorlog" tot "De oorlog van de toekomst wordt bepaald door critical data deletion". Deze benadering omvat zowel de civiele als militaire hoek en is "volkomen nieuw".
- *Klassiek militair*: information warfare is het verlengde van (verbindings)-inlichtingen (SIGINT) en (verbindings)beveiliging. Informatie over een tegenstander is noodzakelijk om de strijd succesvol te kunnen voeren. Hierbij wordt vrijwel alleen de militaire kant in een traditioneel conflict benaderd en blijft de niet-militaire kwetsbaarheid van civiele infrastructuren buiten beschouwing.
- De laatste groep is globaal gesproken een *synthese* tussen de eerste twee hoofd-stromen. Het zwaartepunt richt zich hier op modelvorming. Zowel de klassieke als de meer speculatieve technieken krijgen een plaats in een model. Hierbij zijn de modellen toepasbaar of hebben betrekking op zowel de militaire als de civiele wereld. In het vervolg van dit rapport zal uitgegaan worden van deze benadering.

Daarnaast gebruikten of misschien wel misbruikten veel auteurs de term Information Warfare, terwijl de definitie daarvan nog hoogst onduidelijk was of zelfs nog is. Hierdoor is Information Warfare soms ten onrechte gelijk gesteld aan een bepaalde invalshoek. Vanaf 1996 wordt de term "Information Warfare" echter generiek gebruikt als het overkoepelende element van een aantal, deels klassieke, technologieën, technieken en doctrines.

Begin 1997 ontstond de ontwikkeling dat men vooral in de Verenigde Staten van de politiek beladen term "oorlog" in "Information Warfare" af wilde. Tenslotte is informatie verzamelen en het gecoördineerd verspreiden van informatie (bijv. psychologische druk) niet voorbehouden aan de militairen ten tijde van oorlog alleen. Het is ook ten tijde van 'peacekeeping', tijden van oplopende spanning, en allerlei vormen van conflict van belang. In het militaire domein valt het plannen en de inzet van middelen onder operatiën, vandaar dat sinds medio 1997 de term "Information Operations" (Info Ops) zijn intrede deed en daarna heel snel en breed geaccepteerd is. Information Warfare als term wordt nu voor twee doeleinden gebruikt: 1) als aanduiding van het gehele "vakgebied", 2) als aanduiding van het tactische deel van Info Ops tijdens een conflict, in Amerikaanse termen "de slagveld term voor Information Dominance" (zie Figuur 2.3, Figuur 2.4 en Figuur 2.5). In de US Joint Chiefs of Staff Joint Pub 3-13, 'Joint Doctrine for Information Operations' [JP3-13] van 9 oktober 1998 [JP3-13] is dit geformaliseerd.

## 2.3 Klassen van Information Warfare

Om het IW-onderzoeksveld enigszins te structureren is het zinvol de verschillende verschijningsvormen van IW in groepen of klassen in te delen. Vergelijkbaar met de vele definities van IW zijn er ook op het gebied van indeling verschillende voorstellen gedaan. Hierbij geldt in hoge mate dat de voorstellen voor ordening sterk afhankelijk zijn van de visie van de betreffende auteur en de "school" waartoe hij behoort. Een aantal verschillende indelingen zal worden behandeld. In de volgende hoofdstukken worden deze indelingen in één model bijeengevoegd.

### 2.3.1 Information Warfare indeling volgens Libicki

Libicki [Lib] onderscheidt zeven vormen van IW. Deze zijn:

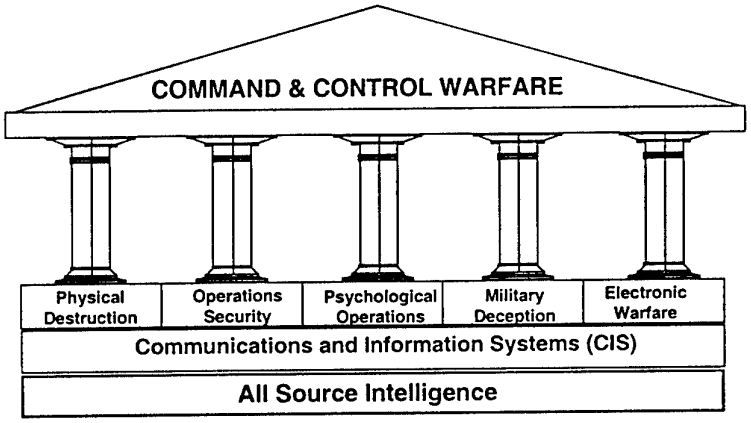
1. Command-&-Control Warfare (C2W): aanvallen van C2-systemen en informatievoorsprong opbouwen,
2. Intelligence-based Warfare (IBW): aanvallen gebaseerd op het gebruik van all source intelligence,
3. Electronic Warfare (EW): (on)mogelijk maken van C2W en IBW,
4. Psychological Warfare (PSYW) en Operations (PSYOPS): zowel civiele als militaire psychologische beïnvloeding,
5. Hacker Warfare: voornamelijk op civiele en infrastructurele doelen,
6. Economic Information Warfare (EIW): economische spionage en (real-time) al dan niet versluierde informatieverstoring of -blokkade,
7. Cyber Warfare: voornamelijk gericht op strategische infrastructuur.

De eerste drie zijn niet nieuw en bestaan al in een of andere vorm en zijn ook veelvuldig in conflicten gebruikt. Wel is het zo dat door de vooruitgang van de technologie de verschijningsvorm zich wijzigt, aanpast of uitbreidt.
Psychologische oorlogvoering is niet specifiek of uitsluitend een militaire aangelegenheid. Sommigen zetten bij de term "oorlogvoering" voor de categorieën 5-7 hun vraagtekens, vooral omdat deze categorieën ook betrekking hebben op zaken buiten de directe militaire invloedssfeer.
Als met "oorlogvoering" echter "overwicht op een andere samenleving door offensieve acties en of drukmiddelen" bedoeld wordt, dan is deze terminologie zeer wel juist.

#### 2.3.1.1 Command and Control Warfare (C2W)

Voor Command and Control Warfare (C2W) hanteert de Amerikaanse defensie twee verschillende definities (zie bijlage B). Eén waarbij ook de civiele C2-infrastrastructuur die door defensie gebruikt wordt deel van uit maakt en een andere definitie van de Joint Chiefs of Staff (beperkt tot militaire operaties):

- De Amerikanen beschouwen C2W (Command & Control Warfare) als een militaire strategie die Information Warfare toepast samen met fysieke vernietiging. Het doel is om de commandostructuur van de opponent uit te schakelen en zo de uitvoerende krachten ineffectief te maken.
- In de civiele wereld is "C2" aan de orde bij die infrastructuren die de overheid in brede zin gebruikt voor de aanpak van calamiteiten, rampen en ernstige verstoringen van de openbare orde.




*Figuur 2.1: NATO Command & Control Warfare (C2W) structuur*

Nederland gebruikt de NATO C2W definitie:

> *The integrated use of all military capabilities including Operations Security, Military Deception, Psychological Operations, Electronic Warfare and Physical Destruction; supported by all source intelligence and communication and information systems; to deny information to, influence, degrade or destroy an adversary's C2 capabilities while protecting friendly C2 capabilities against similar actions. Also called C2W'*

Figuur 2.1 stelt deze NATO C2W definitie dit visueel voor. Deze figuur kan misleidend werken. De C2W aspecten zijn geen separate peilers, doch zijn aspecten die in interactie samen het C2W "dak" dragen.

Offensief kunnen er twee mogelijke C2W tactieken uitgewerkt worden:

- *Het vernietigen of uitschakelen van de centrale leiding ("Anti-head").*
  - Het uitschakelen van de centrale leiding is een al eeuwen oude aanpak. Een aantal aspecten dat hierbij bedacht moet worden is:
    - Hoe identificeerbaar is de centrale leiding?
    - Hoe centraal is centraal, d.w.z. is er geografische spreiding en is er sprake van back-up/alternatief?
    - Welke vrijheidsgraden bezitten de uitvoerende eenheden en hoe flexibel zijn zij?
    - Hoe hecht is de band tussen leiding en uitvoerende ofwel hoe goed gehoorzamen lagere echelons aan de leiding en hoe vrij zijn zij in hun resultaatgericht handelen?
  - Deze methode is soms niet zo effectief meer: commandanten zijn fysiek eenvoudig te verplaatsen. Commandoposten zijn (in de toekomst) mogelijk niet zo makkelijk meer te identificeren.
  - Enkele Information Warfare mogelijkheden: computervirussen, uitschakelen stroomtoevoer, elektromagnetische impulsen, uitpeilen (*EW bijdrage aan C2W*), informatie-overload en spoofing.
- *Het uitschakelen van de verbindingen tussen leidinggevende en uitvoerende (Anti-neck").* Aspecten die van belang daarbij zijn, zijn:
  - Kennis van de infrastructuur van de tegenstander en de daarin aanwezige redundantie, zowel geplande als toevallige;
  - Positieve of negatieve controle van de centrale sturing;
  - Flexibiliteit en vrijheid van handelen van uitvoerende eenheden;
  - Mate van integratie die noodzakelijk is voor effectiviteit.

  Bij een aanval op de verbindingen van een tegenstander kan het voordelig zijn verbindingen niet geheel te verbreken maar slechts te beperken (degrading) zodat de mogelijkheden van een tegenstander om te reageren beperkt worden. Voorbeelden: knooppunten die communicatielijnen verbinden, brandstof pijpleidingen, zendmasten, jamming.

Het vernietigen van beveiligde verbindingen is juist wel een geschikt doelwit omdat zo een tegenstander gedwongen wordt om onveilige verbindingen te gebruiken die mogelijk gemakkelijker zijn af te luisteren.

Welke aspecten ook beschouwd worden om effectief te kunnen opereren op het terrein van C2W, er dienen drie vragen beantwoord te kunnen worden:

- Waaruit bestaat de infrastructuur van de tegenstander?
- Hoe wordt deze infrastructuur gebruikt in termen van sturing en gestuurd worden?

- Hoe moet de aan te brengen of aangebrachte schade beoordeeld worden (Battle Damage Assessment) en is deze BDA te controleren?
  Over het gebruik van zogenaamde softkill wapens dient in dit opzicht niet te lichtvaardig te worden gedacht, een bomkrater is goed waarneembaar, de effectiviteit ervan beoordelen is moeilijker, een virus in een netwerk of informatiesysteem is nauwelijks waarneembaar ("is een deel van zijn functie") om over de (zichtbare) effectiviteit maar te zwijgen.

Defensief dienen de C2-infrastructuren beschermd te worden. Zaken als diversiteit, redundantie, *minimum essential* (defence) *information infrastructure* (ME(D)II), vermindering van kwetsbaarheid en afhankelijkheid zijn dan van belang.
Door de opkomst van Information Warfare zullen commandanten nu explicieter kosten, vertragingen, onzekerheden en de complexiteit m.b.t. de informatie--infrastructuur moeten leren inplannen.

#### 2.3.1.2 Intelligence-Based Warfare (IBW)

Traditioneel is inlichtingen een zaak van waarnemen en verzamelen gevolgd door bewerkings- en analyseprocessen waarna de inlichtingen beschikbaar komen voor gebruik. Bij gebruik moet hier gedacht worden aan Command & Control (C2). Een bevelhebber is in staat, om op basis van verkregen inlichtingen, zijn krachten te bundelen, de tegenstander te verrassen en te voorkomen dat hij zelf verrast wordt.

Bij Intelligence-Based Warfare worden de inlichtingen/informatie direct gebruikt in de operationele sfeer, dit wordt ook wel genoemd een sensor to shooter interface. Doel hier bij is om de OODA loop (zie paragraaf 4.1) te verkorten door een deel van de processen te automatiseren. Denk hierbij aan meer sensoren waarvan de gegevens met behulp van bijvoorbeeld data-fusie gecombineerd worden tot een totaal beeld van het slagveld. De verkregen waarnemingen worden direct gebruikt om tot actie over te gaan, zonder of met beperkte menselijke inbreng.

##### 2.3.1.2.1 Offensieve Intelligence-Based Warfare

Het doel van offensieve Intelligence-Based Warfare is het optimaal en maximaal inzichtelijk maken van het strijdtoneel en de ondersteunende processen, acties, motivaties en psychologie.

##### 2.3.1.2.2 Defensieve Intelligence-Based Warfare

De defensieve variant van IBW is er op gericht om eigen middelen voor een tegenstander zoveel mogelijk af te schermen. Bij beide "varianten" hoort ook het gebruik van misleiding (deceptie) en desinformatie om tegenstanders het zicht op eigen mogelijkheden- en onmogelijkheden te ontnemen, waarbij in de OODA-cyclus (observe, orient, decide, act cyclus) van de tegenstander een verkeerde beslissing of actie genomen wordt gebaseerd op misleidende informatie (zie ook paragraaf 4.1).

### 2.3.1.3 Electronic Warfare (EW)

De eerste twee varianten van Information Warfare zijn globaal gesproken gericht op het aanvallen van systemen (C2W) of het aanvallen met of door systemen (IBW). Electronic Warfare omvat de militair tactische (civiel: operationele) offensieve en defensieve mogelijkheden hiervan.

EW technieken worden gebruikt om communicatie te verstoren, te beveiligen en/of te gebruiken als informatiebron om dreigingen vroegtijdig te lokaliseren. EW valt dan ook uiteen in Electronic Attack (EA) middels Electronic Counter Measures (ECM), Electronic Protection (EP) onder andere door Electronic Protective Measures (EPM) en Electronic Counter-Counter Measures (ECCM) en Electronic Support (ES) middels Electronic (warfare) Support Measures (ESM).
Enkele technieken:

- anti-radar en anti-communicatie, onder andere: jamming, frequency hopping, spread-spectrum;
- cryptografie: versleutelen van boodschappen of kraken van versleutelde boodschappen. Het decoderen van versleutelde berichten is bijna onmogelijk, met name in real-time. (DES, PKE, RSA). Het gebruik van digitale technieken maakt het zich voordoen als een ander (spoofing) bijna onmogelijk. Digitale handtekeningen kunnen de integriteit en authenticiteit van berichten garanderen.

Op het raakvlak van Electronic Warfare en CyberWar vallen ook de totaal nieuwe "future" wapens als High Power Microwaves (HPM) en High Energy Radio Frequency (HERF) guns om elektronische circuits in systemen "op te blazen".

### 2.3.1.4 Psychological Warfare (PSYW en PSYOPS)

Bij psychologische oorlogsvoering zijn vier categorieën te onderscheiden:

- nationale gedachtenvorming (bijv. perceptie van chaos bij het ineenstorten van een kritische infrastructuur),
- tegen de commandovoering van de vijand,
- tegen troepen (bijv. angst voor dood),
- cultureel conflict (bijv. perceptie van cultuur van 'de ander').

Technologieën: TV (de "CNN-factor" wordt inmiddels als belangrijke publieke opinie-invloed gezien), radio, Internet, Digital Broadcasting System (DBS).

Voorbeelden:

- Voor en tijdens de Kosovo-crises is PsyOps nadrukkelijk gebruikt. Opvallend beeld was "Mrs. Albright", die Servië via CNN publiekelijk een laatste kans gaf om Rambouillet te tekenen. Ze had daarbij een witte (vredeskleur) shawl om en had een opvallend grote broche op in de vorm van een (vredes)duif.
- Door de directe terugkoppeling van tactische operaties met life-beelden, bijv. CNN, kan zowel de eigen zaak als die van de opponent door een tactische actie ineens een wending krijgen op operationeel en ook strategisch niveau. De

beelden van de tactische overwinning van de Amerikanen in Mogadishu werd als "geheim" achtergehouden; het beeld van de tegenstander die met het lichaam van een dode Amerikaan rondgingen[3] veroorzaakte de beslissing op Amerikaans strategisch niveau op zicht terug te trekken.

Nieuwe media en het gebruik daarvan kunnen dus een enorme psychologische invloed hebben. Goed omgaan hiermee vergt opleiding, training en geld. [4]

#### 2.3.1.5 Hacker Warfare (HackInt)

Vaak wordt onder Hacker Warfare het kraken van computers verstaan (zie o.a. [WSchw]). De bedoeling van zulke "kraken" kan zijn:

- platleggen of verstoren van systemen en infrastructuren,
- informatiediefstal,
- aantasten integriteit van de informatie,
- ongeoorloofd gebruik van diensten (bijv. gratis telefoneren),
- monitoren en verzamelen informatieverkeer (intelligence)

Militaire doelen zijn *soms* (zie ook §5.7.5.1) beter beveiligd en zijn in een aantal gevallen fysiek losgekoppeld van publieke netwerken. Militaire aanvallen op informatie systemen vielen onder C2W en IBW, maar zijn nu onderdeel van Info Ops.

Civiele en overige overheidssystemen, netwerken en infrastructuren kunnen worden aangevallen op drie niveaus: *fysiek*: zie C2W; *semantisch*: veranderen van de inhoud die computers ontvangen van elders (zie Cyberwar); *syntactisch*: bitverplaatsing.
Een andere indeling betreft die in:

- *kerndoelen*: elektriciteit, gas/olie, water, telecommunicatiebasisinfrastructuur;
- *functionele doelen*: de basisinfrastructuur voor andere diensten (bijv. mobiele netwerk, luchtverkeersleidinginfrastructuur, spoorwegennet);
- *randsystemen*: toegevoegde waarde systemen waarvan de uitval vervelend is, doch vitale functies van de samenleving niet direct in gevaar brengt (bijv. betaalautomaten, radio, TV, 112-systeem, beurssystemen).

Dit werpt de volgende open vragen op:

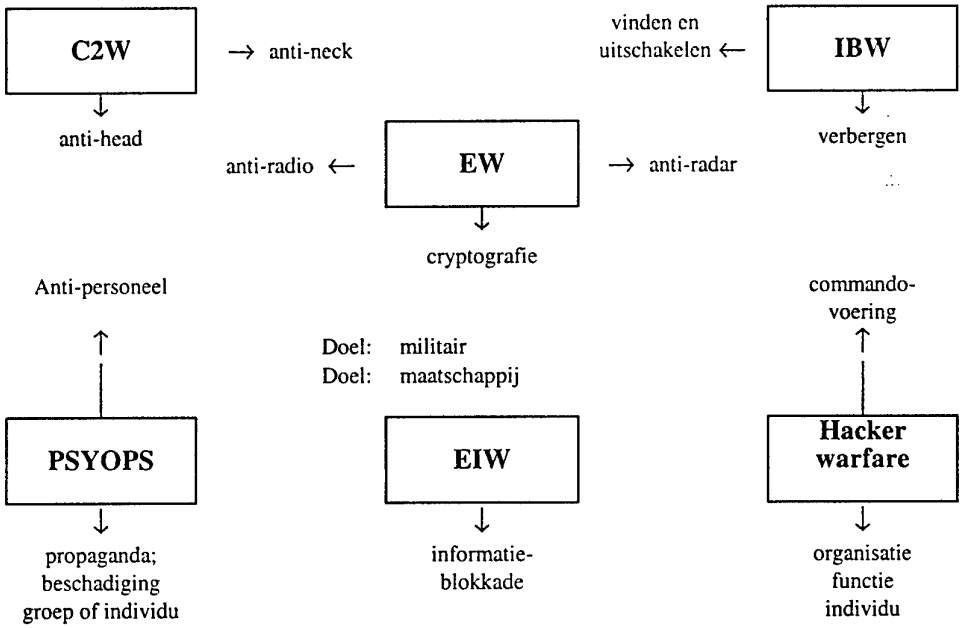
- Hoe zijn op commercial-off-the-shelf (COTS) gebaseerde systemen en netwerken eenvoudig beter te beveiligen?
  (belangrijke militaire systemen zijn veelal zodanig ontworpen dat zij "aanvallen" kunnen afslaan; de COTS-tendens doorbreekt dit principe)

---

3 CNN heeft overigens het naakte lichaam van de soldaat via beeldmanipulatie een onderbroek aangetrokken.

4 In de NL-DU studie Information Operations komen de psychologische aspecten aan de orde in hoofdstuk 6 "The Human Aspects". De onderliggende studie door TNO-TM, aangevuld met technische aspecten vanuit TNO-FEL, is in een TNO-TM rapport [Kleij99] vastgelegd.

- Hoe is te voorkomen dat aanvallen op publieke systemen, netwerken en infrastructuren de politiek en de overheid afleiden van nationale defensietaken?
- Hoe is de kwetsbaarheid te verminderen van kritische civiele / emergency managementssystemen, die niet zodanig ontworpen zijn dat zij "aanvallen" kunnen afslaan?
- De vraag is wat voor maximale schade een alleen werkende "hacker" eventueel zou kunnen aanrichten, zoals het platleggen van (deel van) een nationale telefonie-infrastructuur. Waarschijnlijk is het effect hiervan minder dan van een grootschalige natuurramp (bijv. aardbeving, overstroming).
- Moet er door de Staat aandacht aan defensieve hacker warfare worden besteed? Moet je de "onschuldige" huishacker laten lopen en alleen aandacht besteden aan de echte aanvallers?
- Moet er door de Staat der Nederlanden aandacht aan offensieve hacker warfare (counter-warfare) worden besteed?




*Figuur 2.2: Indeling van Information Warfare aspecten (uit [Bosch97b] naar Libicki)*

### 2.3.1.6 Economic Information Warfare (EIW)

EIW richt zich ten eerste op de financieel-economische infrastructuren. Informatieblokkade, het blokkeren van informatiestromen in en uit een land, zou een middel kunnen zijn. EIW zou in de toekomst een land kunnen treffen zoals nu een goederenblokkade of boycot dat kan. Een informatieblokkade is echter alleen effectief voor real-time informatie. Als er een fysieke blokkade is, wordt de effectiviteit groter. De effectiviteit van een informatie blokkade is afhankelijk van het landsbelang in communicatie.

In het civiele domein vallen onder EIW ook economische spionage en bedrijfs-spionage. Naar verwachting vormen deze aspecten van EIW een steeds belangrijker bedreiging. Hierbij is nauwe verwantschap met hacker-activiteiten.

#### 2.3.1.7 Cyber of Cybernetic Warfare (CyberWar)

CyberWar (of Cybernetic Warfare (CYW)) en NetWar zijn volgens sommigen nog "futuristische" vormen van Information Warfare, sterk gericht op de samenleving (civiele infrastructuur) en politiek alsmede de economische infrastructuur. Beide vormen zijn gericht op de strategische structuur. CyberWar omvat ook psychologische "oorlogsvoering" terwijl NetWar zich alleen richt op de informatie-infrastructuur.

Naar een schatting uit 1997 hebben meer dan 100 landen potentieel de mogelijkheid om *gestructureerd* aan CyberWar te doen, daarvan bedreigen er zo'n 50 de westerse wereld. Nog eens 25 landen hebben ondergrondse "hacker"-groeperingen welke mogelijk uit zijn op het uitbuiten van CyberWar of NetWar mogelijkheden. [5]

Onder Transnational Infrastructure Warfare (TIW) is een gecombineerde vorm van NetWar en Economic Warfare, waarbij de infrastructuur van sleutelindustrieën en -bedrijven in een (deel van een) land aangevallen worden.

### 2.3.2 Information Warfare indeling volgens Magsig

De indeling van Magsig [Magsig] is gebaseerd op een achttal principes die een rol spelen in de Information Warfare. Deze indeling is een uitwerking van die welke is voorgesteld door Jensen [Jens] en heeft voornamelijk betrekking op de militaire "wereld". De acht principes of uitgangspunten worden ingedeeld in vier categorieën van twee principes. Deze categorieën zijn:

- De categorie van *verhindering of belemmering* bestaat uit de principes van:
  - **Decapitation:** een tegenstander is niet meer in staat zijn eigen resources effectief te besturen.
  - **Sensor primacy**: het vermogen ontzeggen aan een tegenstander om vrijelijk waarnemingen te doen.
- De categorie *force enhancement*: sterkte of krachtmultiplicator:
  - **Kennisvergaring** en **kennisdistributie** waarbij er voor gewaakt wordt dat de juiste en voldoende kennis op het juiste moment aanwezig is daar waar hij gebruikt wordt.
  - **Alacrity of tijdigheid** dit wil zeggen dat er een korte beslissingsprocedure is en dat voor elk handelen een zekere mate van urgentie bestaat. Informatie heeft soms slechts gedurende een beperkte tijd waarde!

---

5 Op 10/12/1997 is een CyberWar poging gedaan m.b.t. de dagelijks zeer vaak geraadpleegde Yahoo-website. Alleen tegen vrijlating van de hackers-'martelaar' Mitnick zou een trojan horse die via Yahoo op vele systemen terecht zou zijn gekomen, kunnen worden gedeactiveerd.

- De categorie van het *behoud van overzicht en interventie* bestaat uit:
  - **Overleving (survivability)** vereist dat het politiek-strategisch niveau centraal en dat het operationeel niveau en het tactisch niveau decentraal uitgevoerd wordt. Dit vereist een overgang van het hiërarchisch model naar een netwerkmodel. Iedereen kent het totale plaatje en kan in geval van nood (geen contact met naast hogere) zelfstandig handelen.
  - **Samenwerking (interoperability)** het (kunnen) delen van informatie dient maximaal te zijn. Dit speelt zeer beslist een rol bij samenwerking tussen verschillende organisaties.
- De categorie van de *verschillende niveaus en inzet* bestaat uit:
  - **Niveau,** dit dient hier gezien te worden als mogelijkheden welke deel uitmaken van het wapenarsenaal.
  - **Inzet (intensity)** heeft betrekking op het gegeven dat elke confrontatie op elk niveau met alle inzet van middelen gerealiseerd dient te worden.
    Ook vereist het dat beleidsmakers zich onthouden van beïnvloeding van het operationele en tactische niveau.

### 2.3.3 Information Warfare (HackInt/CyberWar) indeling volgens Winn Schwartau

Winn Schwartau is een informatiebeveiligingsspecialist. Zijn visie op IW komt dan ook vanuit de informatiebeveiligingshoek (InfoSec) en is met name op HackInt/CyberWar gericht. Hij beschrijft in [WSchw] een indeling in drie klassen van IW:

- Class 1: ***Personal*** Information Warfare
  Beschrijft aanvallen op de persoonlijke elektronische privacy. Veel persoonlijke informatie is opgeslagen in centrale databases die gevoelig zijn voor fraude.
  Voorbeelden: Creditcard-nummers, medische gegevens, persoonlijke financiële gegevens.
- Class 2: ***Corporate*** Information Warfare
  Deze groep beschrijft de informatie-concurrentiestrijd (war) tussen bedrijven. Voorbeeld is industriële en economische spionage.
- Class 3: ***Global*** Information Warfare
  Hieronder valt "*informatieterrorisme*".

### 2.3.4 Information Warfare indeling volgens Bgen. Prof. Bosch (KMA)

Bgen. Prof. Bosch heeft zes van de zeven verschillende door Libicki onderkende vormen van IW, zowel in het militaire als het civiele domein, in een figuur (afgeleid van [Libicki]) samengevat. CyberWarfare wordt door hem nog niet als 'actueel' gezien. Zie Figuur 2.2. Het is echter eenvoudig aannemelijk te maken dat Cyberwar spoedig realiteit wordt, zo niet al is.

## 2.4 Verschillende niveaus van Information Warfare

Het denken en doen wat betreft Information Warfare kan, naar analogie van de klassieke oorlogsvoering, ingedeeld worden aan de hand van de verschillende niveaus waarop IW zich kan afspelen (Joints Chiefs of Staff of the US Armed Forces). Er worden drie militaire niveaus (achtergrond, zie bijlage C) onderkend.[6]

### 2.4.1 Strategisch niveau

Dit is het hoogste niveau ofwel hier speelt nationale veiligheidspolitiek of internationaal bondgenootschap. Hier zal doorgaans sprake zijn van een zogenaamde "Global view". In het uiterste geval zullen alle nationaal ten dienste staande middelen worden aangewend.

Noot: een betreffend conflict kan heel goed regionaal zijn echter het wordt dan gewogen en beoordeeld in relatie tot (alle) andere wereldwijde belangen.

### 2.4.2 Operationeel niveau

Er is sprake van aanzienlijke belangen en grotere eenheden zijn regionaal actief maar de invloed op het grote geheel, b.v. de nationale veiligheid, is beperkt. Veelal zal er sprake zijn van zogenaamde Combined (meer departementen of meer dan twee naties) en/of Joint Operations (meer Krijgsmachtdelen van één land).

### 2.4.3 Tactisch niveau

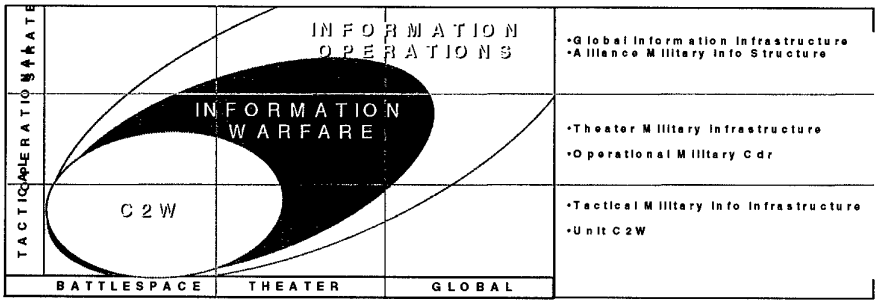
Dit is het laagste niveau van handelen, hier spelen politieke overwegingen geen rol, en worden de korte termijn beslissingen genomen om een voordeel te behalen.

## 2.5 Information Operations (Info Ops)

Zoals al eerder aangegeven, is sinds medio 1997 het denken over Information Warfare sterk opgeschoven van "war" naar (de voorfasen van) "conflicten" en daarmee van "warfare" naar Information Operations. Recentelijk heeft NATO een Info Ops definitie vastgesteld [MCM-069-98]. Die definitie is vrij ruim en wijkt af van die van de Amerikaanse Joint Chiefs of Staff (zie ook paragraaf 3.1). De NATO definitie is echter leidend voor de Nederlandse begripsvorming.
De meest recente gedachten over en daarmee definities over Information Warfare beperken zich tot het operationele en tactische vlak in het militaire theater domein. Information Operations strekt zich tevens uit tot de strategisch en wereld-omvattende (global) domeinen. Figuur 2.3 brengt deze relaties tussen Information Operations, Information Warfare en C2W en de drie militaire niveaus in één figuur bijeen.

---

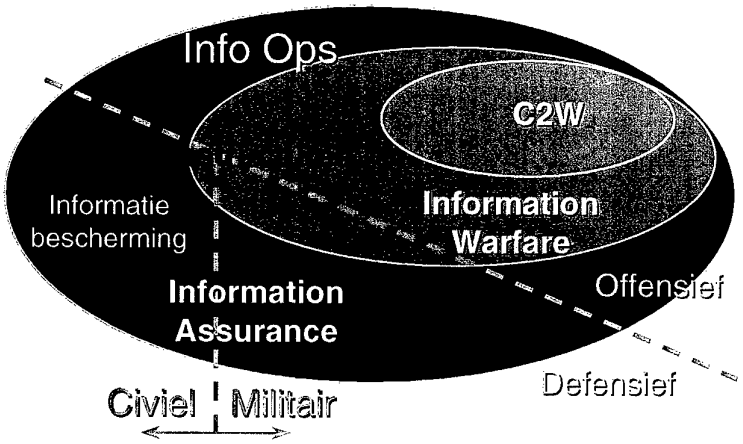
6 In de civiele omgeving worden de termen *operationeel* en *tactisch* in omgekeerde volgorde gebruikt.




*Figuur 2.3: Information Operations [bron: KMA]*

De globalisering van de informatie, informatiemiddelen, informatie-infrastructuren vindt vooral plaats binnen de civiele wereld. Deze ontwikkelingen raken direct de interacties en relaties tussen de militaire en de civiele werelden. Beschouwen we het Libicki-model (zie Figuur 2.2), dan is duidelijk dat offensieve IW direct de samenleving treft. Anderzijds kunnen terroristen en anderen tijdens de ontwikkeling van een conflict zich richten op de emergency management systemen en netwerken, waar de militaire systemen op verzoek van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties deel van uitmaken. Hiermee dringt civiele "IW" binnen in de militaire wereld. Er is daarmee sprake van een overlappend gebied waar zowel voor civiele als militaire defensieve IW een rol weggelegd is.

De overlap tussen de militaire en civiele wereld en de defensieve aspecten die tot uitdrukking komen in Informatiebescherming en Information Assurance worden aangegeven in Figuur 2.4.



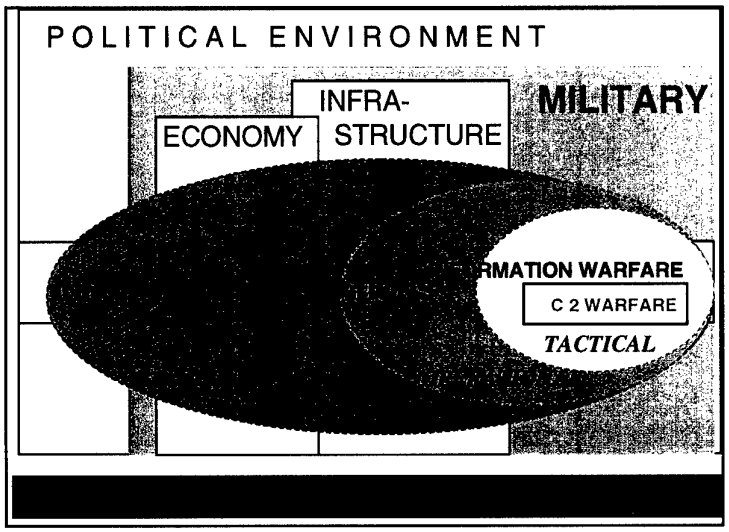

*Figuur 2.4: Info Ops, IA en de militaire en civiele omgevingen*

Tenslotte geeft Figuur 2.5 nog een andere doorsnede van Information Operations. Hierbij zijn de drie militaire niveaus en die van de politieke, economische en (civiel) infrastructurele omgeving aangegeven welke een vrijheid van handelen vereisen (Info Ops defensief), dan wel ontzegd moet worden (Info Ops offensief).

Information Operations ontwikkelt zich hierbij van een hulpmiddel tijdens conflicten ("force multiplier") naar een middel dat zelf als "force" ingezet kan worden [uitspraak Gen. Schoomaker, USCINCSOC].

## 2.6 IW conflictontwikkeling

Indien een conflict zich ontwikkelt, zal er sprake zijn van een verschuiving qua inspanning en aandacht voor de verschillende IW-aspecten (uit het Libicki model). Een mogelijke ontwikkeling en verschuiving van Information Operations naar Information Warfare wordt in Figuur 2.6 in beeld gebracht.




*Figuur 2.5: Spectrum van Information Operations [bron: KMA]*

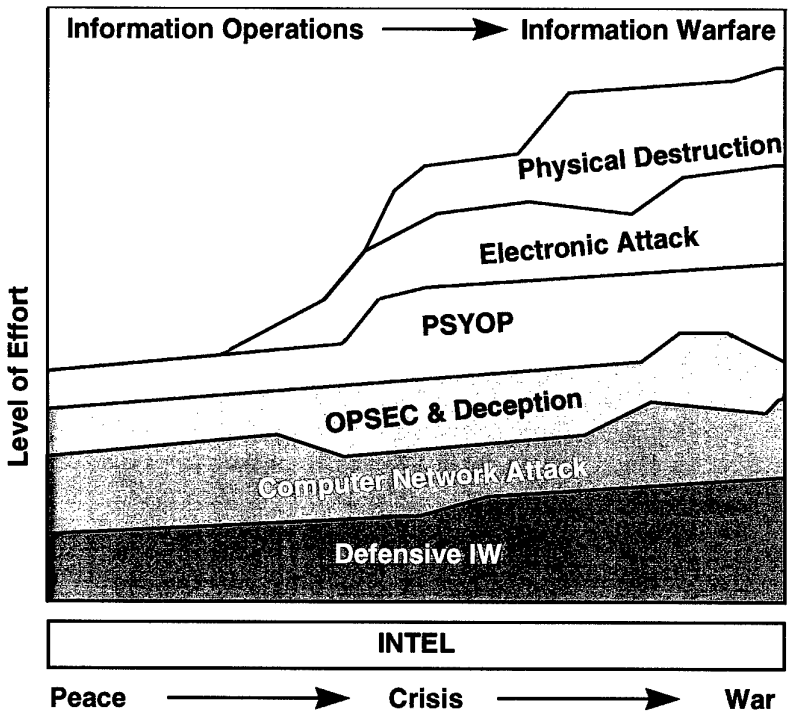
## 2.7 Elementen van offensieve Information Warfare

Offensieve Information Warfare heeft dezelfde aspecten als andere vormen van warfare in zich. Tot de aanvalsmogelijkheden behoren: deceptie, verstoren, ontzeggen van vrije toegang of volledig lamleggen (denial-of-service), gebruik maken van opponentsystemen en infrastructuren voor eigen doeleinden, vernietiging.

*Offensieve systemen* dienen een aantal van de volgende eigenschappen te hebben:

- *Penetratie*: zich toegang verschaffen tot de systemen en/of infrastructuren van de opponent;
- *Heimelijk* (stealth): verhinderen van detectie of identificatie van de aanvalsbron;
- *Imitatie*: de mogelijkheden om zich zo voor te doen dat het authenticatiesysteem van de opponent zonder detectie of identificatie toegang verleent (spoofing, trojan horse);

- *Zichtbaar resultaat*: na een aanval moet het offensieve systeem de mogelijkheid hebben om de effecten en resultaten van de aanval te kunnen beoordelen.
- *Doeltreffend:* resultaat met minimale inspanning is wenselijk.




Source: Derived from a Joint Staff pamphlet, titled, "Information Warfare,"undated.

*Figuur 2.6: Voorbeeld van een IW-conflictontwikkling*

## 2.8 Elementen van defensieve Information Warfare

Defensieve Information Warfare probeert de aanvalsmogelijkheden van een tegenstander te blokkeren, de effecten van eventuele aanval te minimaliseren. Bovendien is het van belang (heimelijke) acties van een tegenstander zo vroeg mogelijk te detecteren en waar mogelijk tegenacties te initiëren.

*Defensieve systemen* dienen de volgende eigenschappen te hebben:

- *Training en preventie*: voorbereiding op het bieden van tegenstand;
- *Detectie*: vroegtijdig onderkennen van verkenningen en aanvallen door een opponent;
- *Redundantie*: de gevolgen van een aanval door een opponent te minimaliseren door extra systemen;
- *Hardening*: systemen en infrastructuren bestendig maken tegen aanvallen;
- *Monitoren en controle*: continu nagaan of de veilige situatie van informatie en informatiesystemen nog steeds gehandhaafd is;
- *Deceptie*: verwarren van een mogelijke opponent.

Opvallend is dat de Amerikanen uitgaan van een beperkter model: *protectie*, *detectie* en *reactie*. Al is er veel theoretisch en praktisch onderzoek gaande naar detectie, het blijkt heel moeilijk om zogenaamde "cyber attacks" te kunnen onderscheiden van "normale" storingen in een systeem (bijv. een MS Windows crash).

## 2.9 Attitude en Information Warfare

Voor alle elementen die in een conflict een rol spelen, geldt dat er bij elk offensief aanwenden van een techniek een defensieve techniek voorhanden is dan wel ontwikkeld zal worden.

> *De meest paradoxale defensieve techniek is het dreigen met maar het niet gebruiken van offensieve mogelijkheden. Op een aantal terreinen van IW kan dit wel eens de enige mogelijke defensieve techniek blijken te zijn.*

Dit zou vergelijkbaar zijn met het MAD (Mutual Assured Destruction) principe dat de nucleaire wapentechnologie beheerst. Hierbij dient de volgende kanttekening te worden gemaakt: het MAD-principe werkt en werkte het best tussen gelijkwaardige partijen die een zelfde aanval- en verdedigingaanpak hebben. Wanneer de partijen ongelijkwaardiger worden, zal de zwakste partij waarschijnlijk minder te verliezen hebben. Bij de nucleaire technologie werd dit gecompenseerd door het vermogen van de sterkste partij(en) om de verspreiding van deze kennis en technologie te beperken, *non-proliferatie*. Tegelijkertijd is er sprake van herkenning van de tegenstander en kunnen controlemechanismen overeengekomen worde.

Het MAD-principe is echter *niet van toepassing voor informatietechnologie* omdat het de relatief goedkope technologie van "om de hoek is". MAD kan dus alleen werken voor een beperkt deel van het IW-spectrum.

Toch gaan er stemmen op dat het juiste gebruik van de Information Operations middelen: open source intelligence; effectief ICT-gebruik en elektronische veiligheid en counter-intelligence kan leiden tot "Information Peacekeeping" [Steele98], waarbij een conflict in de kiem gesmoord wordt.

De belangrijkste conclusie die uit het voorgaande getrokken kan worden is dat:

> Een samenleving die in hoge mate afhankelijk is van het correct functioneren van zijn informatiesystemen, informatievoorzieningen en infrastructuren zich er niet aan kan onttrekken om op Information Warfare gebied actief beschermende maatregelen te treffen.

## 2.10 Op weg naar één eenduidige definitie

Het terrein van de information warfare, information operations en information assurance is zowel in de militaire als de civiele wereld op dit moment nog een heterogene verzameling van begrippen en verschijnselen. Er zijn twee aspecten die dit duidelijk illustreren:

- het nog niet geheel uitgekristalliseerd zijn van eenduidige definities (in bijlage B zijn een aantal definities opgenomen),
- de grote inhoudelijke verscheidenheid van publicaties op het IW-terrein.

De reden hiervoor is hieronder aangegeven bij de bespreking van het Nolan fasenmodel (paragraaf 2.11).

Wanneer de definities overzien worden zijn de volgende zaken op te merken:

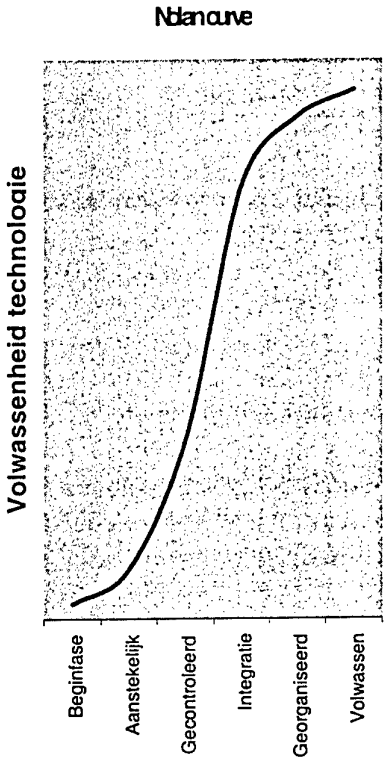
- Veelal zijn de definities afkomstig uit de militaire wereld.
- Sommige zijn zo ruim opgesteld dat bijna alles er onder verstaan kan worden zodat de waarde betrekkelijk is.
- De eerste definities waren voornamelijk gebaseerd op de opsomming van een aantal technieken.
- Informatie en systemen worden in een adem genoemd; infrastructuren worden nog al eens minder belicht.
- Het in 1997 ontstane begrip 'Information Operations' is met weinig discussie geaccepteerd door de NAVO-landen. Hierdoor ontstaat inmiddels een steeds beter begrip en daarmee definitie van wat onder Information Operations verstaan moet worden.

## 2.11 Het Nolan-model en de ontwikkeling van IW

In 1973 ontwikkelde R.L. Nolan een model voor de ontwikkeling van ICT-technologie. Hij onderkent daarin een S-vormige curve met 6 fasen. Vergelijkbare fasen blijken in alle technologie-ontwikkelingen onderkend te kunnen worden. Na een beginfase met zogenaamde pioniers, werkt de technologie of "het idee" aanstekelijk voor "early adopters". Daarna gaat de technologieontwikkeling snel met sprongen voorwaarts, waarbij de inbedding en het gebruik van de technologie in organisaties op gecontroleerde(re) wijze gaat dan in voorgaande fasen.
Daarna ontwikkelt zich de fase waarin de technologie geïntegreerd wordt met andere technologieën. Er treedt een grote wijziging op in de wijze waarop de technologie strategisch ingezet wordt door de organisatie. Geleidelijk wordt de technologie via de fase van georganiseerd gebruik volledige ingebed in de strategische denk- en werkwijze van de organisatie.
Vanuit de "fase van volwassenheid" ontstaat de overstap naar een andere technologie S-curve, waarbij soms een sprong optreedt.

*Voorbeeld communicatiemedia*
De radio ontwikkelde zich vanuit een pioniersfase naar de aanstekelijkheidsfase waarin de eerste families buren en vrienden zich om de radio kluisterden. In de gecontroleerde fase werd

de radio een 'must' voor het consumentenpubliek, waarbij omroepen ontstonden met programmavulling. Daarna nam de radio de taak van actuele nieuwsvoorziening over en werden nieuwe 'formules' bedacht' (hitparades). Vanuit de volwassen midden- en kortegolf-technologie, wordt de technologie nog steeds stapsgewijs verbeterd: via FM, stereo en RDS naar digitale radio. Geheel parallel hieraan was de sprong naar de volgende Nolan S-curve van de televisie welke de zich nog steeds ontwikkelende, maar geheel volwassen technologie van de radio niet geheel kan verdringen.




*Figuur 2.7: Nolan curve van technologieontwikkeling*

Als we dit Nolan model betrekken op Information Warfare in brede zin, dan wordt duidelijk dat vele landen zich in de beginfase van IW bevinden, daarbij aangestoken door de "early adopter" Amerika. Te onderkennen valt dat de technologieontwikkeling zich nog in de beginfasen van de S-curve bevindt, waarbij de ontwikkelingen zeer snel gaan, de richting nog vaag is, maar waarbij wel snel een focus en consensus ontstaat van wat de technologierichting mogelijk kan betekenen c.q. welke gevaren die herbergt. Er is zowel sprake van een technologie-push door early adopters of nieuwe bedrijven in de commerciële wereld als een technologie-pull vanuit afnemerszijde.

Tevens wordt dan duidelijk waarom er momenteel nog vele definities voor de term "Information Warfare" in omloop zijn (zie hoofdstuk 3 en bijlage B). Toch blijkt uit de literatuur en de afnemende discussies hierover tijdens de gevolgde IW-conferenties dat de definities en gedachten over wat IW is door voortschrijdend inzicht snel naar elkaar toekomen.

# 3. Definities

Zoals in het vorige hoofdstuk is aangegeven, is er de laatste periode een duidelijkere focus aan het ontstaan wat de definitie van Information Warfare, Information Operations en Information Assurance. De Verenigde Staten heeft door voortschrijdend inzicht en ook om politieke terminologie redenen sinds eind 1996 de brede term "Information Warfare" los gelaten ten faveure van Information Operations en Information Assurance.

De term "Information Warfare" wordt in inmiddels als overkoepelende paraplu-term voor het gehele technologie- en doctrine-'speelveld' gebruikt. Daarnaast wordt de term Information Warfare gebruikt als aanduiding van het tactische deel van Info Ops tijdens een conflict (zie Figuur 2.3, Figuur 2.4 en Figuur 2.5). Omdat dit laatste een sterke overlap met C2W heeft, is deze terminologie nog minder in gebruik. Als zodanig zal de term IW ook in het vervolg van dit rapport in generieke zin gebruikt worden, tenzij expliciet anders aangegeven.

## 3.1 Information Operations (Info Ops)

Nederland en Duitsland gaan uit van de NATO-definitie van Information Operations [MCM-069-98] in de gezamenlijke Info Ops studie: [7]

> *Actions taken to influence decision makers in support of political and military objectives by affecting other's information and/or information systems while exploiting and protecting one's own information and/or information systems. There are two main categories of Info Ops: defensive Info Ops and Offensive Info Ops, depending upon the nature of the actions involved.*

Information Operations omvatten politieke overheids- en militaire activiteiten ter benutting en bescherming van de eigen informatie-omgeving om gestelde (bijv. strategische) doelen te bereiken, waarbij aanvallen op de informatie(systemen) en infrastructuren van de opponent een optie is. De Amerikaanse definitie stelt daarnaast dat zij voorsprong en overwicht nastreven. Kanttekening vanuit de andere NATO-landen is, dat de voorsprong en het overwicht die men kan krijgen beperkt is qua omgeving, omvang en tijd. Daarnaast is definitie is nogal ruim en vaag.

Deze definitie omvat dus drie aspecten: 1) offensieve inzet, 2) effectief gebruik en 3) defensief gebruik van eigen informatie en informatiemiddelen. Aspect 2), ook wel Info Info Ops genoemd, richt zich sterk op het management van de eigen informatie. Omdat dit een ruim gebied omvat en binnen Defensie barrières kan opwerpen (bijv. discussie BIS- non-BIS (CIS)), concentreert de Nederlandse defensie zich eerst op de defensieve Info Ops: de zo goed mogelijke bescherming

---

7 Dit zal in de gezamenlijke NL-DU studie nader uitgewerkt worden.

op alle aspecten tegen verstoring en aanvallen. Vergelijk dit met een beschermende schil om de informatiesystemen en infrastructuren heen. Om de eigen bescherming goed te kunnen controleren zullen offensieve Info Ops middelen nodig zijn (bijv. een hackers (red) team).

Aan de offensieve kant staat het de Nederlandse Defensie vrij om te kiezen welk(e) middelen zij wil ontwikkelen en inzetten. In bondgenootschappelijk verband zal er op dit terrein ook afstemming nodig zijn om te kunnen beschikken over een zo breed mogelijk palet aan opties.

## 3.2 (US) Information Assurance (IA)

De medio 1997 in de Verenigde Staten ingevoerde term Information Assurance is daar als volgt gedefinieerd:

*Information Operations that protect and defend information and information systems by ensuring their:*

- *Availability,*
- *Integrity,*
- *Authentication,*
- *Confidentiality and*
- *Non-repudiation.*

*This includes providing for the restoration of information systems by incorporating protection, detection and reaction capabilities.*

Deze definitie bevat de beschrijving van veel informatiebeveiligingsaspecten, doch is niet uitputtend. Gemist worden onder andere aspecten als: controleerbaarheid, identificatie alsmede de bescherming van infrastructuren.

## 3.3 Informatiebescherming (Information Assurance)

Bovenstaande definitie van Information Assurance is met name voor de niet-militaire wereld minder aansprekend en niet bruikbaar. Onze ambitie is dat ook aan de bescherming van de kritische infrastructuren van de Nederlandse Staat en de kritische economische infrastructuur van BV Nederland nadrukkelijk veilig gesteld wordt. Hierom is de volgende definitie voor Informatiebescherming (Information Assurance) door ons opgesteld:

**Informatiebescherming (Information Assurance)** *is het beschermen van:*

- *de (Nederlandse) Staat,*
- *de samenleving,*
- *haar economische nationale en internationale belangen,*
- *haar bondgenoten en supranationale organisaties,*

*tegen de effecten van aanvallen op en verstoringen van:*

- *informatie,*
- *informatie-verwerkende processen,*
- *informatiesystemen,*
- *informatie-infrastructuren, en*
- *essentiële infrastructuren en diensten.*

## 3.4 Information Warfare (IW)

Sinds eind 1996 is de term Information Warfare in de Verenigde Staten beperkt tot [8]:

*Information Operations conducted during time of crises or conflict to achieve or promote specific objectives over a specific adversary or adversaries.*

Inmiddels heeft ook NATO een voorgestelde definitie van Information Warfare in engere zin. Deze is nog niet bekrachtigd en is ook nog niet door de Nederlandse Defensie geaccepteerd:

*Offensive and defensive Information Operations conducted during time of crises or conflict to achieve or promote specific political or military objectives over a specific adversary or adversaries.*

Deze definitie sluit het efficiënt gebruik van de eigen informatie als derde aspect van Info Ops uit. Het staat ter discussie of dat wel zo bedoeld is.

## 3.5 Command & Control (Information) Warfare (IW-C2W)

Nederland gaat uit van de NATO-definitie van Command & Control Warfare (C2W). Voor de volledigheid en ter vergelijking met de voorgestelde NATO-definitie van IW is ook deze definitie hier opgenomen:

*The integrated use of all military capabilities including Operations Security, Military Deception, Psychological Operations, Electronic Warfare, and Physical Destruction; supported by all source intelligence and communication and information systems; to deny information to, influence, degrade, or destroy an adversary's C2 capabilities, while protecting friendly C2 capabilities against similar actions.*

---

8 Zie eerdere discussie op pagina 15 over het begrip Information Warfare in bredere en in engere zin.

## 3.6 Information Peacekeeping

De definitie van Information Peacekeeping is ontleend aan [Steele98]:

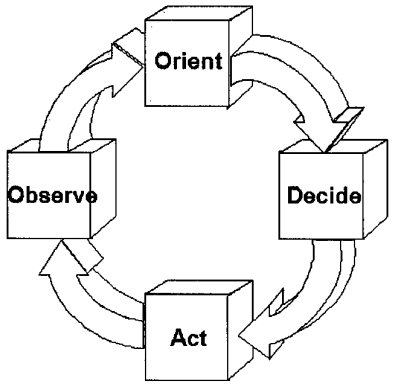
*Information Peacekeeping is the active exploitation of information and information technology so as to achieve national policy objectives. The three elements of Information Peacekeeping, in order of priority are open source intelligence; ICT-technology; and electronic security and counter-intelligence.*

# 4. De (model)wereld van Information Warfare

## 4.1 De OODA-cyclus

Een veel gehanteerd model voor procesbeschrijving in de militaire wereld (in het bijzonder in de luchtmacht) is de zogenaamde OODA cyclus of OODA-loop. Deze staat voor:

**O**bservation - het waarnemingsproces
**O**rientation - het evaluatieproces
**D**ecision - het besluitvormingsproces
**A**ction - het uitvoerende proces




*Figuur 4.1: De OODA-cyclus*

Dit model is ook buiten de militaire wereld bruikbaar om "handelingen" te beschrijven of te analyseren. De laatste actie zal in het algemeen een reactie tot gevolg hebben, waarna de gehele cyclus opnieuw doorlopen zal worden.
De OODA cyclus is zowel bruikbaar voor de beschrijving van zowel menselijk als niet menselijk handelen of een combinatie van beide:

- *Observatie* is het proces van het verzamelen van kwantitatieve gegevens (metingen).
- De *oriëntatiefase* is de fase waar het gevecht om de geest en wil van de tegenstander plaatsvindt. Hier zou beïnvloeding plaats kunnen vinden door zoiets bizars als een virtual reality fenomeen. Uitgaande van het feit dat de beslissing in de geest van een tegenstander het doel is van IW-PSYOPS, is het gevechtsterrein van de menselijke geest ook het gebied van de illusie. [Stein]
- *Decision*: op basis van de eigen ' Common (consistent) understanding of the battlespace ' wordt een beslissing genomen om de eigen doelstellingen te bereiken. Het decision-proces omvat ook het formuleren, plannen, evalueren, gezamenlijk bespreken (collaborative planning) en het uiteindelijk kiezen van de uit te voeren optie, inclusief alternatieven.

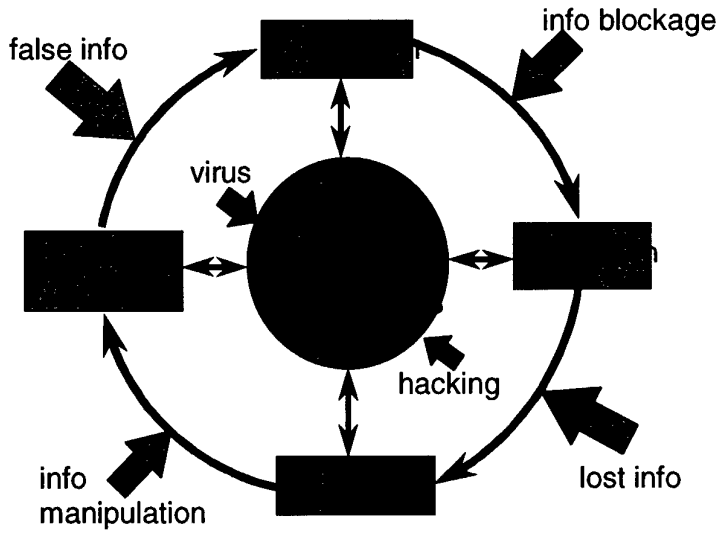
- Action: vervolgens worden acties ondernomen om de genomen beslissing te realiseren.

De tijd die beschikbaar is om de OODA cyclus te doorlopen is afhankelijk van het niveau waarop hij uitgevoerd wordt. Op het laagste tactische niveau is de beschikbare tijd minimaal, hier kan de meeste winst geboekt worden met "automatisering" het implementeren van een sensor-to-shooter interface.

IW in termen van de OODA cyclus is het verkorten van de eigen OODA cyclus/cycli (ten koste van) en het uitrekken, verstoren of verwarren van de OODA-cyclus van de tegenstander. De eigen cyclus wordt sneller doorlopen dan die van de tegenstander waardoor die achter gaat lopen en geen tijd meer heeft om adequaat te reageren.

Probleem met dit model is, dat vele militaire processen hun eigen "klok" hebben. Van cycli die zich in een seconden voltrekken tot processen die uren zo niet dagen vergen. Het afstemmen van de informatieprocessen op elkaar bij een joint en combined operatie en het behalen van winst vergt het kunnen aanpassen en schalen van de drijvende klok van de kritische processen ('major tick').

In het licht van offensieve en defensieve Information Operations kunnen we van twee kanten de OODA cyclus bekijken. Enerzijds van buiten af: hoe is de cyclus te verstoren en te frustreren? Van binnenuit kunnen we nagaan waar een tegenstander mogelijk offensief zal willen aanvallen. Daar dienen we ons defensief te wapenen en eventueel tot tegenacties over te kunnen gaan. Een model hiervan met een aantal (niet uitputtend) offensieve dreigingen is getekend door de KMA (Figuur 4.2).[9]

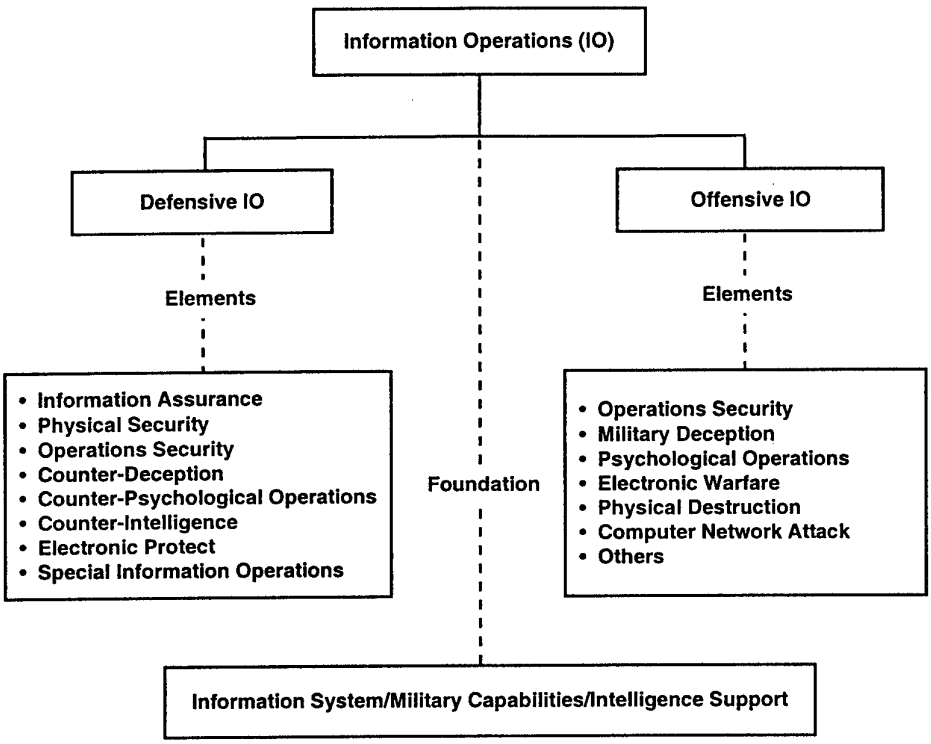



*Figuur 4.2: Kwetsbaarheden van de OODA-loop [bron: KMA]*

9 Een uitgebreide discussie over de menselijke factor, de OODA-loop en Info Ops is te vinden in het TNO-rapport (Kleij99].

## 4.2 Information Operations (Info Ops) hiërarchisch model

Het Information Operations (Info Ops) hiërarchisch model (Figuur 4.3) is ontwikkeld door het US Institute for Defense Analysis (IDA) [IDA97].




*Figuur 4.3: Information Operations hiërarchisch model [IDA97]*

## 4.3 Conflictenmodel

Het conflicten- en dreigingsmodel uit Figuur 4.4 werd door Ed Waltz gepresenteerd tijdens het HSA IW-seminar [HSAEW]. Vervolgens werd aangegeven op welke wijze offensieve en defensieve Information Warfare binnen die verschillende typen conflicten tot uiting komen.

Defensie houdt zich traditioneel met name bezig met het militaire C2W domein. De aanvaller met NetWar/CyberWar mogelijkheden is een bedreiging voor een groot scala aan militaire, publieke infrastructuur en civiele, economische doelen. Aanvallers uit de $2^e$ en $4^e$ categorieën kunnen vanuit overal in de wereld toeslaan. Het vooraf bekend zijn van de dreiging, het traceren en de identificatie is daardoor zeer moeilijk.

Guerrilla oorlog

| | | Hoog technologisch niveau | Laag technologisch niveau |
|---|---|---|---|
| Economische oorlogen | **Fysiek conflict** | 1. Militair C2W<br>• hoge intensiteit slagveld<br>• economische macht<br>• precisiedoelen<br>• heimelijkheid: fysiek<br>• C4I technologie | 3. Guerrilla oorlogsvoering<br>• lage intensiteit slagveld<br>• zonder mededogen<br>• random doelen<br>• natuurlijke heimelijkheid<br>• menselijke netwerken (als technologie); omvat ook narcoticaconflicten |
| | **Abstract conflict** | 2. NetWar, CyberWar<br>• Cyberspace conflict<br>• kennis-macht<br>• gegevensbanken als doel<br>• IT-heimelijkheid<br>• wereldwijde netwerken (als technologie) | 4. Ideologische oorlogsvoering<br>• ideologisch, religieus of etnisch conflict<br>• ideologische macht<br>• aanval op massa/samenleving<br>• ideologische heimelijkheid<br>• ideologische netwerken |

Terrorisme

Culturele oorlog

*Figuur 4.4: Vier typen conflict, uitgesplitst naar categorie en benadering*

*Tabel 4.1: Information Warfare mogelijkheden per type conflict [HSAEW]*

| | Offensieve IW | Defensieve IW |
|---|---|---|
| Militaire C2W (1) | • EW deceptie, verstoring, uitbuiten<br>• precisie-aanval op C2-nodes en infrastructuur<br>• Psyops<br>• Netwar aanvallen | • ECM<br>• InfoSec<br>• ComSec<br>• vinger aan de pols houden (intelligence) |
| NetWar, CyberWar (2) | • systeempenetratie<br>• code met neveneffecten<br>• uitbuiten van systemen en gegevens<br>• informatiecorruptie - perceptie van het management | • InfoSec<br>• CompuSec<br>• ComSec<br>• vinger aan de pols houden (intelligence) |
| Guerrilla oorlog (3) | • propaganda<br>• penetratie van organisaties<br>• media en sociale controle<br>• cellenstructuur | • fysieke beveiliging<br>• vinger aan de pols houden (intelligence) m.b.t. culturele ontwikkelingen en ontwikkelingen in samenleving |
| Ideologische oorlogsvoering (4) | • ideologie via ether verspreiden<br>• cultureel en politieke medestanders vinden | • vinger aan de pols houden (intelligence) m.b.t. ideologische ontwikkelingen in samenleving<br>• Open, all source intelligence (OSCINT), COMINT |

## 4.4 IW en militaire disciplines

| | Observatie | | | | Beslissen | Informatie Aanval | Informatie Verdedigen |
|---|---|---|---|---|---|---|---|
| | Voorbereiding | Verzamelen | Verwerken | Verspreiden | Bevelen | Aanvals informatie | Verdedigings informatie |
| **Intelligence** | IPB<br>MASINT<br>IMINT | ← - - -<br>HUMINT<br>RADINT<br>OSCINT | | - - - →<br>FISINT<br>TELINT<br>IMINT | | | |
| **InfoSecurity** | | | | | | **Offensieve Info Ops?** | |
| **Electronic Warfare** (EW) | | | | | | | |
| **Command and Control** (C2) | | | | | | | |
| **Special Operations** | | | | | | PSYOPS special Ops | |
| **Cyber Operations** | | | | | | CyberOps | |

*Figuur 4.5: Militaire Information Warfare functies en militaire disciplines*

Een andere kijk op Information Operations levert de doorsnede van militaire functies en disciplines verdeeld over voorbereiding/beleid, observatie, beslissen (en beslissingsondersteuning), informatieaanval en informatieverdediging.[10]

Verschillende deskundigheidsgebieden binnen TNO (FEL, TM en STB) dekken tezamen het grootste deel van dit spectrum af:

- Assistentie bij het opstellen van Info Ops beleid en doctrine.
- Analyse en simulatie van Info Ops capabilities en de wijze waarop deze ingezet kunnen worden;
- C4I architectuur en design, informatie-analyse, development en ondersteuning;
- Sensortechnologieën en data fusion;
- Visualisatie van de informatiestromen en systeem assurance status;
- Human factor aspecten van de beslissingscyclus;
- EOV met name op het gebied van SIGINT en (ver)storing;
- Communicatie als (veilige) drager;
- Informatiebeveiliging en fysieke beveiliging, inclusief Red, Green en Blue team

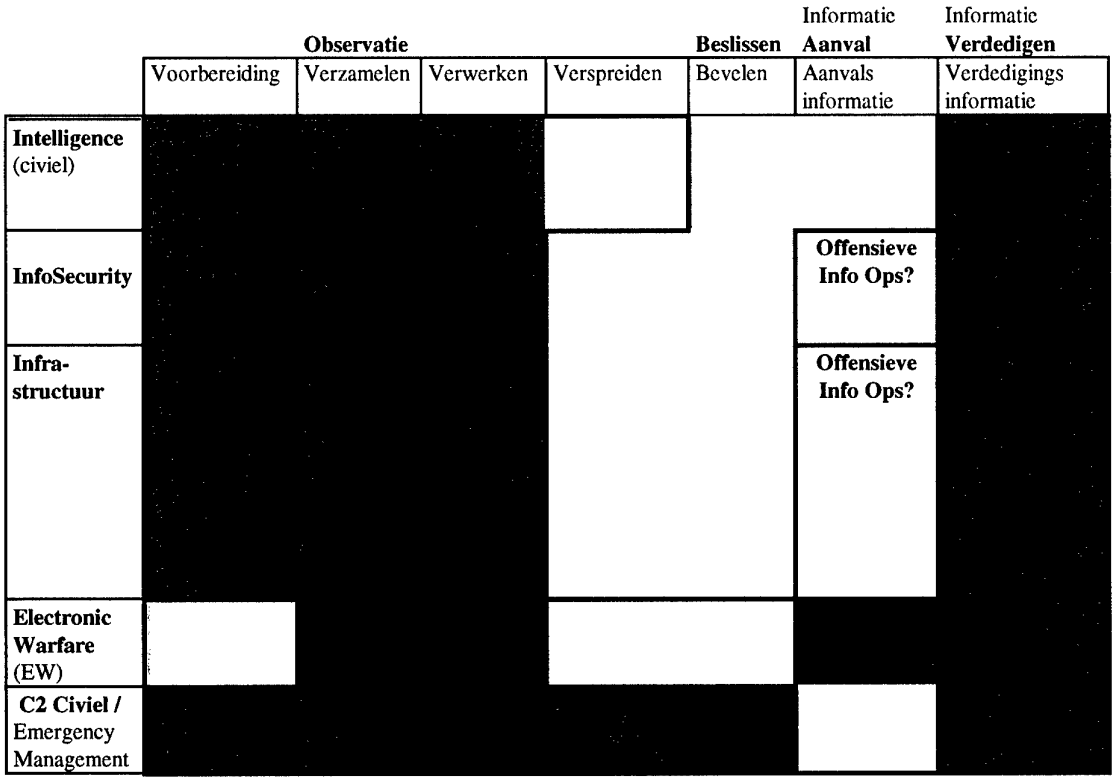
[10] Op EW-gebied wordt door NATO alleen gesproken over Electronic Protection, Support en Counter Measeures (EPM, ESM en ECM). Voor de volledigheid zijn ook de elders in gebruik zijnde termen in de figuur genoemd.

activiteiten;[11]
- Training en opleidingsmethoden en hulpmiddelen;
- Red/Green team activiteiten (heimelijk resp. openlijk aanvallen eigen informatie infrastructuur);
- Optimaal gebruik van systemen;
- PsyOps (deels).

In hoeverre Info Ops *offensief* binnen Defensie gebruikt gaat worden, hangt af van de operationele randvoorwaarden welke uit de NL-DU studie naar zullen voren komen. Offensief blijft een keuze waarbij de opties die potentiële coalitiepartners hebben een rol meespelen. Defensief zal het totale spectrum afgedekt moeten worden.

## 4.5 IW en civiele aspecten

Figuur 4.6 bevat een vergelijkbaar overzicht als dat in Figuur 4.5, maar nu voor IW en de civiele informatie-infrastructuren.



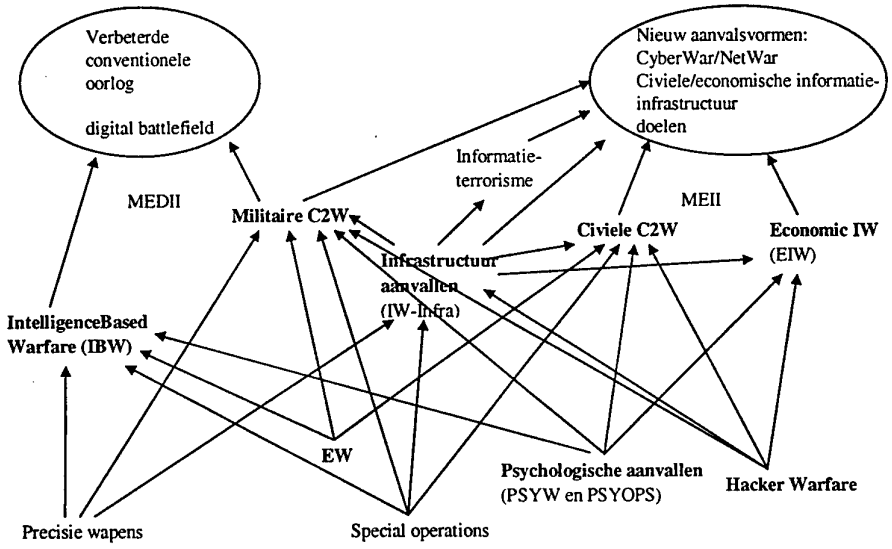

*Figuur 4.6: Information Warfare functie, zowel civiel als militair*

[11] Een Red Team verricht heimelijk testen in het eigen netwerk ter controle van de defensieve status. Een Green team doet dat openlijk. Het Red team kan een "Blue team" worden, indien de aanwezige kennis ingezet wordt om een "aanval" door derden te analyseren en af te wenden (assistentie CERT).

Hierbij zijn wederom de Information Operations aspecten van voorbereiding/beleid, observatie, beslissen (en beslissingsondersteuning), informatieaanval en informatieverdediging als horizontale indeling genomen. Op vrijwel alle onderkende, in de figuur gekleurd aangegeven gebieden, is TNO in staat om vanuit haar domein- en technologiekennisgebieden de overheid en het bedrijfsleven te ondersteunen bij het veilig stellen van onze kritische economische belangen. Denk hierbij bijvoorbeeld aan de ondersteuning bij beleidsontwikkeling en de technische aspecten van Information Assurance voor wat betreft de civiele bescherming (bijv. emergency managementdiensten als politie en brandweer) en de bescherming tegen "cyber-aanvallen" op kritische infrastructuren en diensten.

Als we de aanvalsmogelijkheden in relatie brengen met de doelen, dan komen de in Figuur 4.7 aangegeven onderlinge relaties naar voren. Zo kunnen precisie-wapens ingezet worden op basis van IBW kennis tegen specifieke doelen van de tegenstander, kunnen de militaire C2-infrastructuur of de commandoposten aangevallen worden of kan de totale (kritische) infrastructuur aangevallen worden.

## 4.6 De IW-vormen en dreigingen in één beeld tezamen




*Figuur 4.7: De IW-aanvalsvormen op doelen in het militaire en het civiele domein*

# 5. Information Warfare, de internationale situatie

## 5.1 Australië

Door het Australisch Strategic and Defence Studies Centre (ASDSC) is in 1997 een studie [ASDSC] uitgevoerd naar de kwetsbaarheid van de National Information Infrastructure. (NII).
Het onderzoek ging uit van een aantal scenario's en heeft deze afgezet tegen geconstateerde kwetsbaarheden van informatie-infrastructuren en de samenleving. In de studie is ook de kwetsbaarheid voor natuurrampen meegenomen. Een aantal markante conclusies:

- De defensie, economische en financiële informatie-infrastructuur van Australië is kwetsbaar. In de door hen opgestelde IW-scenario's blijkt weinig verschil meer te bestaan tussen "warfighters" en "niet-combattanten". Niet alleen blijkt het *verschil tussen militair en civiel vaag* te zijn, maar ook blijkt de Australische samenleving (net zoals alle "westerse samenlevingen" *nauw verweven te zijn met de even kwetsbare wereldomspannende globale informatie-infrastructuur* (GII).
- Omdat de IW-dreigingen nog niet levensbedreigend zijn, is er (nog) weinig politieke aandacht voor, waardoor er ook weinig middelen beschikbaar zijn voor studie naar potentiële conflictdreigingen en het treffen van preventieve maatregelen. *Gebruikelijke defensie-scenario's voldoen niet*, omdat enerzijds de dreigingen van overal uit de wereld kunnen komen en anderzijds omdat er afhankelijkheden zijn door de verwevenheid van systemen en infrastructuren.
- *Nationale veiligheid*, het beschermen van de samenleving en de sociale, politieke en economische structuur, *omvat (daarom) meer dan militair defensie*. Dit is het nieuwe aspect van IW.

De studie noemt een aantal voorbeelden van kwetsbaarheden van de Australische nationale informatie-infrastructuur (NII), welke bestaat uit:

- overheidsnetwerken;
- netwerken tussen banken, beurzen en financiële instellingen;
- publieke utiliteitsnetwerken: communicatie, energiedistributie, luchtvaart-begeleidingssystemen en positiesystemen (bijv.: GPS, ILS);
- netwerken voor hulpdiensten (ambulances, politie, brandweer, reddingsdiensten);
- massacommunicatiesystemen (radio, televisie);
- netwerken van grote ondernemingen;
- onderwijs- en researchnetwerken.

De studie gaat uit van de essentiële kernfuncties voor de samenleving:

- "kern overheidsfuncties" (regering, defensie, buitenlandse zaken en handel, inlichtingendiensten, financiën, sociale zaken en hulpdiensten),

- "kern utiliteitsfuncties" (elektriciteitsnetwerken, telecommunicatie, olieraffinaderijen, gas- en olieopslag en transportsystemen, transport en verkeersbegeleidingssystemen, waterdistributie), en
- "kern commerciële functies" (bancaire en financiële diensten, massamedia, zakelijke systemen en communicatienetwerken).

Veel van deze systemen en infrastructuren - anderen noemen dit de **Minimale, Essentiële (Informatie) Infrastructuur** of **MEII** - zijn van elkaar afhankelijk. Er is bijvoorbeeld energie nodig om communicatiesystemen in de lucht te houden.

Enkele voorbeelden van de geconstateerde kwetsbaarheden:

- De communicatie-infrastructuur kent een aantal kritische knooppunten. Grote steden hebben slechts enkele centrales die alle verbindingen met de "buitenwereld" onderhouden. Er zijn slechts een beperkt aantal onderzeese kabels (overigens heeft Nederland er vijf). Het internationale telefoonverkeer wordt afgehandeld door slechts twee centrales die allebei in Sydney staan. De enige (glasvezel)verbinding van Australië met Japan en Amerika loopt via Hong Kong.
- De onderlinge afrekeningen tussen de nationale Australische banken is uitbesteed aan SWIFT. De nationale bank (Reserve Bank of Australia) maakt dagelijks contact met het SWIFT-netwerk in Brussel om de controle op de balansposities van de banken en de geldstromen te kunnen uitoefenen. Dit proces dient binnen drie kwartier (voor de opening van de beurs) plaats te vinden. De kwetsbaarheid is groot! Price Waterhouse gaf al in 1995 aan dat het SWIFT-netwerk (ruim 275 banken; 2500 miljard dollar aan transacties per dag) kwetsbaar is voor verstoring.
- Sinds 1981 maakt de Australische defensie zoveel als mogelijk gebruik van de openbare telecommunicatie-infrastructuur.
- Bij rampen als grote bosbranden en overvloedige regenval blijken telefooncentrales overbelast, hetgeen vergeleken kan worden met een denial-of-service aanval. Een telefooncentrale was na een overstroming drie weken buiten bedrijf omdat er onvoldoende vervangende reserveonderdelen in voorraad waren.
- Een studie begin 1997 naar de activiteiten van hackers bij ruim 500 grote bedrijven gaf aan dat de externe hackersaanvallen, zowel qua hoeveelheid als qua gebruikte technische kennis, in een periode van 18 maanden aanzienlijk toegenomen waren. Ongeveer de helft was nieuwsgierigheid, maar daarnaast bleek 26% (economische) spionage als oogmerk te hebben.

In 1998 is er een vervolgpublicatie uitgegeven [Cobb98] waarin meer op voorziene kwetsbaarheden van de Australische infrastructuren ingegaan wordt. Onderkend worden infrastructuudreigingen ten tijde van de Olympische Spelen 2000 in Sydney.

## 5.2 Canada

### 5.2.1 Canada: Info Ops research

Canada heeft in 1997 een eerste Information Operations research programma opgestart, dat als "Thrust 5.b Information Operations" op de DND website genoemd wordt http://www.crad.dnd.ca/program/thrusts/ccis2_e.html). Onder thrust 5.b vallen 7 projecten die voornamelijk betrekking hebben op Electronic Warfare (EW) bescherming en EW informatieanalyse en datafusie. Ook wordt gewerkt aan de bescherming van informatie systemen en -netwerken (zie ook Thrust 5.c, project 5ch m.b.t. netwerkmanagement). Onder het beperkte 1997 budget werd research uitgevoerd naar een geïntegreerde netwerkmanagement/beveiligingscontrole mechanisme onder één informatiebeveiligings-

beleid (per component instelbaar). Dit pakket heet Ironman. Medio 1998 is dit pakket op TNO-FEL gedemonstreerd.
Ook wordt gekeken naar Onion routing (informatie privacy in netwerk); de sterkte/zwakte van bijvoorbeeld PGP (middels EVES) en firewalls (middels fuzzy logic testen).

Binnen het Department for National Defense (DND), Defence Research Establishment Ottawa (DREO) is in de tweede helft van 1998 een Information Operations researchprogramma opgezet voor de komende jaren[12]. Medio 1999 heeft dat geresulteerd in een nieuwe Info Ops branche. Voor de nieuwe activiteiten is, beginnend met 10 FTE's in 1999, een groei tot 25 FTE's in 2000 voorzien. Daaronder valt ook de opzet van een Info Ops laboratorium. Tussen TNO en DREO wordt, in overleg met wederzijdse ministeries van Defensie, gewerkt aan een vorm van samenwerking op gebied van Info Ops R&D.

### 5.2.2 Canada: Militaire Info Ops

In mei 1998 heeft de Canadese Defensie onder de Joint Staff de "Signals" en "Intelligence" operatiën in één Canadian Forces Information Operations Group (CFIOG) o.l.v. Colonel Randy Alward en zijn rechterhand Lkol. Al Smith (J6IO) bijeengebracht. De CFIOG is onderverdeeld in:

- Canadian Forces EW Center (CFEWC);
- SIGINT;
- Canadian Forces Information Protection Center (CFIPC);
  Informatiebeveiliging:
  - Het Network Vulnerabilities Assessment Team (NVAT). Dit beoordeelt ook de civiele infrastructuren waar Defensie gebruik van maakt. Dit is een zogenaamd Red Team, dat actief de beveiliging van systemen probeert te breken.
  - Het Computer Incident Response Team (CIRT). Hieronder valt ook een engineering section die werkt aan middelen om zwakheden te detecteren.
- Fysieke (counter) operatiën;
- Communicatiebeveiliging.

Ook de Canadian Army is bezig een Info Ops groep in het leven te roepen.

### 5.2.3 Canada: civiele aspecten

Binnen Canada is er nog geen ministerie verantwoordelijk voor kritische infrastructuren, al wordt er wel over gesproken. Wel wordt er onderzoek naar de dreigingen gedaan in het kader van de G8-activiteiten (zie paragraaf 5.11.2) en is ook de Royal Canadian Mounted Police (RCMP) actief op the gebied van computer-veiligheid.

---

12 Betrokkenen zijn bekenden van TNO-FEL.

## 5.3 Duitsland

Vanwege het Bondsstaat-karakter van Duitsland komen de IW-activiteiten nogal verdeeld en grotendeels ongecoördineerd over. Ministeries, krijgsmachtdelen en industrie laten ongecoördineerd parallel verschillende IW/IA studies uitvoeren.

### 5.3.1 Duitsland: BundesMinisterium der Verteitigung (BMVg)

Verschillende beleidsstudies zijn gebaseerd op de Libicki-modelaanpak. Dit heeft geleid tot een IW-beleid, dat nog geaccordeerd moet worden. De Duitse Defensie heeft een wat afwijkende insteek; zij stellen dat het bereiken van militair informatieoverwicht op grotere schaal niet mogelijk is. Wel kan men tijdelijk en plaatselijk een informatieoverwicht bewerkstelligen. In de lange Duitse definitie van IW (bijlage B) staat het verkrijgen en houden van vrijheid van beslissen en handelen centraal. Hierbij worden vier basisvormen van handelen onderkend:

- gebruik van programmatuur,
- gebruik van optische en elektromagnetische middelen,
- gebruik van psychologische mogelijkheden,
- gebruik van wapens en substanties.

Voor de militaire IW is er een IW-definitie die gericht poogt informatieoverwicht te bereiken door zowel offensieve als defensieve maatregelen en acties. Dit omvat ook C2W en het tijdelijk of permanent 'uitschakelen' van de civiele infrastructuur die militair van betekenis is voor de opponent. Een en ander is vastgelegd in een bijna onleesbaar, 1000 pagina's groot document: de "Streitkräfteeinsatz 2020 [SKE 2020]".
De Duitse defensie maakt veel gebruik van openbare netwerken (ook satellieten) en is daardoor kwetsbaar voor Information Warfare.

In november 1998 werd door het Deutsches Gesellschaft für Wehrtechnik een IW-conferentie georganiseerd met als titel: "Chancen und Risiken des Faktors Information - Auswirkungen auf Politik, Gesellschaft, Wirtschaft und Militär". De Duitsers geven daarbij aan dat informatie-superioriteit voor hun belangrijk is en dat organisaties of overheden vanuit de gehele wereld voor weinig geld een bedreiging kunnen gaan betekenen. Het IABG[13] kijkt onder andere naar de Duitse NII en de risico's die de Duitse Defensie daardoor loopt.

Door de "Bundeswehr, dienst materieel" (BWB Koblenz) zijn technische studies gestart naar indringerdetectie in informatiesystemen en -structuren. Ook wordt door het BWB een onderzoek aangestuurd naar de kwetsbaarheden van militaire netwerken (AID - adaptive intrusion detection; TU Cottbus).
Vallend onder de WTDs is bij het WTD Greding recentelijk een defensiebrede registratie van beveiligingsincidenten opgezet onder de naam ZALSA.

---

13 Industrieanlagen-Betriebsgesellschaft mit beschrankter Haftung.

### 5.3.2 Duitsland: civiele aspecten

Het Duitse Bundesministerium des Inneren heeft eind 1997 aan de andere ministeries gevraagd om te komen tot een gezamenlijke aanpak van het onderwerp Information Warfare. Het Zentrale Bundesamt für Sicherheit in die Informationstechnik treedt op als coördinatiepunt. (BSI) [Dbund], [DWT97, blz 18]. Onderkend is dat in Duitsland een IW-strategie naast Defensie ook medewerking van Binnenlandse Zaken, Justitie, EZ en 'Bildung und Forschung' vereist.
Onder leiding van het BSI is de Aktion Gruppe KritIS - werkgroep kritische infrastructuren - aan het werk om in navolging van de PCCIP[14] in de Verenigde Staten (zie §5.7.3.2) na te gaan waar de kwetsbaarheden van de Duitse infrastructuren liggen. De blauwdruk van het rapport moest eind 1998 gereed zijn, waarna de verschillende ministeries delen zouden moeten invullen. Het eindrapport moet medio 1999 gereed zijn.[15] Daarin lijkt vertraging ontstaan te zijn omdat coördinatie binnen de Duitse overheidsstructuur om politieke redenen zeer moeizaam van de grond komt. Samenwerking met publieke partners verloopt nog moeizamer.

Duitsland ziet overigens niets in een gezamenlijke Europese Unie aanpak.

Een eerste bijproduct van de AG KritIS is een campagne om de beveiliging van Internet Service Providers omhoog te krikken. Deze campagne is medio september 1998 gestart.

### 5.3.3 Duitsland: overige onderzoeksinstituten

Onderstaande gegevens zijn ontleend aan informatie die door Dr. Willi Stein (FGAN) in juni'98 in het NATO AC/323 committee gepresenteerd is.

- Institute for Applied System Science and Operations Research (IASFOR), Munchen. Contact: Prof. R.K. Huber, voorzitter van de Federal Armed Forces University.
  Hier worden de militaire aspecten en uitdagingen van IW onderzocht in het licht van externe veiligheid.
- Het Zentrale Bundesamt für Sicherheit in die Informationstechnik (BSI) heeft een baseline informatiebeveiliging op CD-ROM uitgebracht. Het pakket maakt gebruik van Java. Een Engelse versie is in voorbereiding (http://www.bsi.bund.de).
- Forschungsgesellschaft für Angewandte Naturwissenschaften e.V. (FGAN)
  Is dit jaar gestart met het opzetten van een Information Assurance/ Info Ops programma dat zich voornamelijk op de IT-aspecten zal richten.[16]

---

14 (US) President's Commission on Critical Infrastructure Protection.

15 Informatie van Mw. Marit Blattnet-Zimmerman, Leitende Regierungsdirektorin bij het BSI en voorzitter AG KritIS (info 9/98 tijdens InfoWar'98).

16 Contactpersoon is bekend samenwerkingspartner van TNO-FEL.

- Commerciële firma's: Competence Center Informatics (CCI), Meppen; DASA Dornier, Friedrichshafen en IABG München.[17]

## 5.4 Frankrijk

Er is bij ons weinig bekend over Franse activiteiten op dit gebied anders dan binnen NATO en het deelnemen van medewerkers van Dassault aan het IW-seminar in Londen.
Aan de operationele zijde is sinds 1 september 1993 de BRGE - Intelligence and Electronic Warfare Brigade (Brigade de Renseignement et de Guerre Electronique) actief.

## 5.5 Noord-Europa (Denemarken, Finland, Noorwegen, Zweden)

De noordelijke Europese landen zijn voor hun militaire communicatie voor een groot deel afhankelijk van de civiele communicatie-infrastructuur die door de publieke netwerkoperators geboden wordt. Daarom bestaat er in die landen veel belangstelling voor het onderwerp "Defensieve Information Warfare".
De samenwerking tussen de vier genoemde landen op het R&D gebied schijnt echter moeizaam te verlopen.

### 5.5.1 Denemarken

Inmiddels is er binnen de Deense Defensie een IW-programma gestart. Ook de Deense officiersopleiding kent een Information Warfare onderwerp. Het onderwerp staat volop in de belangstelling, ook bij het Deense Defensie Research Instituut (DDRE) waar men met een Information Operations en Information Protection studie gestart is. Men kijkt met name naar indringerdetectie en verdediging in de diepte. [18]

### 5.5.2 Finland

In maart 1997 is er een white paper over Information Warfare gepubliceerd door de Finse overheid. Deze studie omvatte naast defensie ook alle andere belangrijke overheidslichamen.

### 5.5.3 Noorwegen

Net als Zweden lijkt er in Noorwegen veel belangstelling bij de Noorse Krijgsmacht te bestaan voor dit onderwerp. Het Noorse defensieresearchinstituut FFI verricht onderzoek naar Information Warfare. Onder andere zijn er projecten gaande op het gebied van:

---

[17] Het IABG had de verantwoordelijkheid voor hoofdstuk 5 van de NL-DU Info Ops studie.

[18] Informatie: DDRE, email 12/12/97, ICB-vergadering 5/98 en NATO AC/323 (NetOnIP) 6/98.

- Het monitoren van wijzigingen in verkeersstromen.
- Indringerdetectie.
- Het achterhalen van de oorzaak van netwerkinterrupties.
- Het robuuster maken van het netwerk (firewalls, proxy servers, MLS, authenticatie).
- Het verstoppen van communicatieverbindingen (IP-header encapsulation, mobile IP).

De middelen zijn echter beperkt.

### 5.5.4 Zweden

Op 12 november 1997 heeft de Zweedse regering bekend gemaakt dat defensie een diepgaande studie C2W voor het einde van 1998 start. De analyse wordt gebaseerd op een C2W doctrine die door de joint EW sectie (o.l.v. Col. Bertel Wennerholm) opgesteld wordt in de loop van 1998. De C2W doctrine zal zich bezig houden met de Zweedse operatiën ter verdediging van de Zweedse natie en ook de ondersteuning van Zweedse troepen bij internationale peacekeeping en humanitaire steunoperaties. Volgens de Zweden is C2W is gericht tegen de perceptie van de tegenstander; EW is gericht tegen systemen.

Separaat is de Zweedse regering een onderzoek gestart dat de ICT-kwetsbaarheid van de Zweedse samenleving in kaart moet brengen. Dit mede naar aanleiding van scenario analyses door het Zweedse researchinstituut FOA, welke vergelijkbaar zijn met die, die door de Rand Corporation in Amerika uitgevoerd worden. Uit de sessies bleek dat verstoring van de Zweedse samenleving mogelijk is met 'relatief eenvoudige middelen'. Het kabinet van de minister president heeft naar aanleiding hiervan aan de Zweedse regering geadviseerd om:

- een strategisch overzicht van het IW gebied te ontwikkelen binnen de overheidsorganisatie om te komen tot eenduidige beeldvorming ("recognised picture") en eenduidige verantwoordelijkheid;
- een coördinatiegroep binnen het kabinet van de minister president te benoemen die de overheidsrol en verantwoordelijkheden vaststelt;
- de mogelijkheden tot cryptografische bescherming van overheids- èn publieke informatie-verwerkende systemen te versterken;
- het orgaan voor Psychologische Bescherming te belasten met het monitoren van media-manipulatie trends.

Er is een overheids-IW-overleg opgezet waarin 7 à 8 overheidsorganen trekkend zijn. Daarnaast zijn er nog zo'n 20 andere overheidsorganen in dit overleg vertegenwoordigd.

## 5.6 Oost-Europa, inclusief Rusland

Analyses van specialisten uit verschillende landen geven aan dat er een aanzienlijk economische spionage dreiging middels aanvallen op informatiesystemen aan openbare netwerken komt vanuit hoger opgeleide informatiespecialisten en 'hackers' uit met name de voormalige Russische staten. De IW-technologie wordt daar goed begrepen. Dergelijke activiteiten lijken gestimuleerd te worden door de 'Russische Maffia'.
Maar ook in de Doema, het Russische parlement is aandacht besteed aan Information Warfare.

Het ontwapeningscomité van de Verenigde Naties kijkt op verzoek van Rusland naar Information Warfare: "new technologies and their impact on disarmament used as examples, *information warfare*, satellite technology and laser technology for defence research." (GA/DIS/3106 9 October 1998). De gedachte erachter is om een "Possible Info Ops use" - verdrag op te stellen, net zoals het internationale satellietverdrag.

## 5.7 Verenigde Staten van Amerika

Duidelijk is dat noch de Amerikaanse defensie, noch de Amerikaanse overheid een eenduidig, gecoördineerd beeld en beleid heeft op het gebied van Information Warfare en (informatie)infrastructuurbescherming. Binnen de Amerikaanse defensie heeft ieder krijgsmachtdeel, de joint staven en de defensieplanners ieder hun eigen definitie van Information Warfare en Information Operations. De IW-aspecten rondom de civiele infrastructuur worden geheel los daarvan beschouwd. Alleen de lange termijn researchprogramma's van DARPA en de Rand Corporation beschouwen beide aspecten. Hieronder wordt iets dieper hierop ingegaan.

### 5.7.1 USA: defensie en krijgsmachtdelen

De Amerikaanse krijgsmachtdelen, het paarse "Joint Command" en het DoD zijn ieder separaat en ongecoördineerd bezig met Information Warfare. Hierdoor zijn er meer definities in omloop (zie bijlage B). Aan de offensieve kant oftewel bij "Information Operations" (Info Ops) staat information superiority voorop. Information superiority volgens [JV2010] is: "the capability to collect, process and disseminate an uninterrupted flow of information, while exploiting or denying an adversary's ability to do the same". Inmiddels staat de beheersing van informatie-overload - al dan niet gestimuleerd door de tegenstander - volop in de belangstelling.

### 5.7.2 USA: Defense Science Board studie

Het Defense Science Board (DSB) heeft een task force een studie laten uitvoeren naar Information Warfare - Defense (IW-D). Het eind 1996 uitgebrachte rapport [DSB96] stelt: "defensie wordt steeds afhankelijker van de defensie informatie--infrastructuur en steeds meer wordt er van uit gegaan dat deze infrastructuur altijd beschikbaar is". Het DSB stelt meer dan 50 acties voor, waarvoor naar schatting M$ 3.000 over een periode van 5 jaar nodig is.

De studie moest nagaan welke en hoeveel Amerikaanse nationale belangen via de nationale informatie-infrastructuur (NII) geschaad kunnen worden en op welke wijze daar defensieve maatregelen voor getroffen kunnen worden. Hoofdlijnen voor procedures, processen, mechanismen tegen en waarschuwingssystemen voor bedreigingen moesten geschetst worden. De relaties tussen overheid en private sector op dit gebied dienden uitgeplozen te worden.

Het rapport geeft eerst een analyse van de "ist"-situatie. Zo'n 60% van de Amerikanen is dagelijks een elektronische "informatiewerker". Een analyse van dreigingen nu en de verwachting voor de toekomst (2005) laat een verschuiving zien naar wijdverspreide mogelijkheden om inbreuken te plegen op de continuïteit van de informatievoorziening en informatie-infrastructuren, ook die van defensie. Daarna geeft het rapport een aantal aanbevelingen voor defensie:

- Kom tot één verantwoordelijke voor Information Warfare - Defense.
- Organiseer Information Warfare - Defense.
- Verhoog de bewustwording.
- Bepaal de infrastructuur afhankelijkheden en kwetsbaarheden.
- Bepaal de dreigingen en de antwoorden daarop.
- Test geregeld de Information Warfare - Defense alertheid.
- Verhoog de (InfoSec en ComSec) drempel (lage kosten, hoge opbrengst).
- Zorg voor een "Minimal Essential Information Infrastructure" (MEII).
- Focusseer de research en ontwikkelingen.
- Los juridische problemen op.
- Participeer volledig in de bescherming van kritische infrastructuren (ook niet-defensie infrastructuren).
- Stel de middelen hiervoor beschikbaar.

Deze aanbevelingen zijn in het rapport in meer detail uitgewerkt.

Voor het begrotingsjaar 1998 trekt de Amerikaanse Defensie M$ 306 uit voor informatiebeveiliging. Dit is 3% van het totale IT-budget en 56% van het IT R&D-budget. Het Huis van afgevaardigden heeft voor de bescherming van het tactisch internet C2, information warfare/operations survivability van C4I EW-systemen, infrastructuurbescherming C2 systemen in Europa nog eens M$ 10 extra uitgetrokken (House report 105-302, juni 1997). In 1999 is voor de komende jaren nogmaals het bedrag voor Information Protection verhoogd met *1.47 miljard dollar* (een soort 'deltaplan' voor informatiebescherming). DARPA is de sturende organisatie voor veel van de R&D gelden die uit dit budget komen.

### 5.7.2.1 USA: Information Operations Office

Begin maart 1998 heeft het Pentagon onder de OASD/C3I[19] (Organization of the Assistant Secretary of Defense) een op Information Operations gerichte nieuwe structuur opgezet. Onder de OASD/C3I vallen de Deputy Assistant Secretary Departments (DASD's) voor:

- Intelligence Department;
- Command and Control, Communications, Computer Intelligence, Surveillance and Reconnaissance (C4ISR) and Space Systems Department;
- Chief Information Officer Policy and implementation Department; en
- Security and Information Operations Department (o.l.v. Christofer Melloa), met zowel offensieve als defensieve doelstellingen (bron: CIWARS 8 maart 1998). Dit department is onderverdeeld in directoraten voor:
  - Information Assurance,
  - Critical Infrastructure protection,
  - Security,
  - Counter-Intelligence,
  - Info Operations Strategy and Integration.

Door een foutje werd door het US Air Force Info Ops centrum in 1997 ingebroken op een Japans Defensie-systeem, dat ook gepenetreerd werd. Om een diplomatiek incident te voorkomen is door Washington zelf naar Tokio gebeld met de excuses.

Aan de ASDC3I rapporteren de Defense Intelligence Agency (DIA), Defense Information Systems Agency (DISA), National Imagery and Mapping Agency (NIMA), National Reconnaissance Office (NRO), National Security Agency (NSA) en de Defense Security Service [bron: Sig0798].

DISA heeft hierbij tot taak de US C4I infrastructuur en de defensie informatie-systemen te beschermen. Het staat ter discussie of deze DISA taak niet in een "subunified command" thuishoort.
DISA is tevens de vertegenwoordiger van defensie in het National Infrastructure Protection Center (NIPC) (zie §5.7.3.3).

De US Air Force heeft een Info Ops centrum vanwaar uit geprobeerd wordt op Defensiesystemen in te breken, wat vaak lukt. Na 'inbraak' laat het centrum een bericht voor de systeembeheerder achter om contact op te nemen.
Het US Special Operations Command (SOCOM) wordt gereorganiseerd om Info Ops beter te positioneren [InfoW98; sessie B1]. Ook zijn bij de US Air Force de Intelligence en Operations delen bijeengebracht (USAF/XOI).

### 5.7.2.2 USA: militaire visie

De verschillende Amerikaanse krijgsmachtdelen hebben studies verricht naar mogelijke conflicten in de toekomst, benodigde (nieuwe) technologische mogelijkheden en benodigde wijzigingen qua organisatie [JV2010; NWVist]. Deze studies over de krijgsmacht in de 21ste eeuw geven vier operationele concepten aan:

---

19 De Chief Information Officer (CIO) is Arthur. L. Money.

- dominant maneuver / global mobility,
- precision engagement,
- full dimensional protection (zowel tijdens vredestijd, tijdens crisisbeheersing en tijdens oorlog),
- focused logistics.

Hiervoor is volledige (informatie) dominantie (intelligence en C2) over het gehele spectrum van de operatie nodig. Dominantie is overigens een niet kwantificeerbare, kwalitatieve conditie die, gebaseerd op een mate van kennis-voorsprong, de eigen vrijheid van handelen omschrijft. De Amerikanen gebruiken veelal in dit verband ook de term "information superiority", een term die wel een kwantificeerbare maat aangeeft [FM 100-6].

Op 9 oktober 1998 hebben de Joint Chiefs of Staff de Joint Pub 3-13, 'Joint Doctrine for Information Operations' [JP3-13] uitgebracht.

De Amerikaanse Rekenkamer heeft in augustus 1998 een kritisch rapport uitgebracht [GAO98-257] dat stelt dat de superiority doelen nog ver weg liggen. Defensie is al 30 jaar bezig om C4ISR te implementeren, ze komen echter niet van de grond. Ook bij de recente, hierboven beschreven organisatiewijzigingen zet de GAO vraagtekens wat betreft de effectiviteit.[20]

Hierop bracht de US National Research Council (NRC) in mei 1999 het rapport "Realizing the Potential of C4I: Fundamental Challenges" uit. [NRC99] Dit rapport behandelt de IST en SOLL situatie van de C4I systemen. Interessante aanbevelingen betreffen de inzet van COTS systemen, Red teams, en het tijdens oefeningen leren dat delen van het C4I systeem onbetrouwbaar kunnen zijn tengevolge van indringers. [NDRC99]

### 5.7.3 USA: civiele infrastructuurbescherming

Er zijn verschillende commissies, die onafhankelijk van het militaire domein hun eigen insteek hebben. Naast langer bestaande comités, onder andere voor telecommunicatie, heeft de President's Commission on Critical Infrastructure Protection (PCCIP) tussen eind 1996 en eind 1997 de combinatie van infrastructuren en hun kwetsbaarheid in kaart gebracht [PCCIP]. Hieronder een overzicht.

#### 5.7.3.1 US Network Reliability and Interoperability Council (NRIC)

De Network Reliability and Interoperability Council (NRIC) heeft eind 1996 gewezen op de kwetsbaarheid van de openbare telecommunicatie-infrastructuur. Daarbij verwezen ze terug naar de National Research Council die in 1989 een rapport uitgebracht heeft met de titel "The Growing Vulnerability of the Public Switched Network: Security Implications for National Security Preparedness".

---

20 Het meest nieuwe C2 systeem GCCS is niet Y2K-bestendig.

In dat rapport werd voorspeld dat "daar waar publieke en private netwerken gekoppeld worden met soortgelijke software, het gehele netwerk kwetsbaar wordt voor vijandige gebruikers indien die een zwakheid ontdekken".

De NRIC wijst er nu op dat het vrijgeven van de telecommunicatiemarkt nieuwe kwetsbaarheden introduceert:

- Onervaren telecom-operators zijn de zwakste schakel qua beveiliging, terwijl de gezamenlijke netwerkbeveiliging daarvan mede afhankelijk is.
- De verplichting om bepaalde (complexe) diensten te leveren (bijv. nummer-portabiliteit). Dit vergt ondersteuning van complexe signalering en introduceert kwetsbaarheid in geval van fouten in de beveiliging.
- Transparantie van telecomdiensten door heterogene netwerken (GSM, PSTN, ISDN) met behoud van beveiliging is complex. Daarbij moet ook nog eens de integriteit van alle tussenschakels in dat heterogene netwerk veilig zijn.
- Hoe moeten beveiligingsincidenten veilig gerapporteerd worden binnen beperkte kring, zonder dat derden het lek kunnen exploiteren.

#### 5.7.3.2 US President's Commission on Critical Infrastructure Protection (PCCIP)

President Clinton heeft op 15 juli 1996 de President's Commission on Critical Infrastructure Protection (PCCIP) [PCCIP] ingesteld met als doelstelling te rapporteren over en aanbevelingen te doen betreffende:

- welke kritische infrastructuren zijn er eigenlijk, wie zijn de eigenaren en welke anderen (overheden, bedrijven, publieke sector) zijn mogelijk geïnteresseerd in de continuïteit van de kritische infrastructuur?
- welke kwetsbaarheden zijn er qua aard en type; wat zijn de dreigingen?
- welke politieke en juridische aspecten zijn er verbonden aan de bescherming van een kritische infrastructuur?
- voorstellen voor beleid en een implementatiestrategie voor de bescherming tegen fysieke en *"cyber"* dreigingen.

Het op 14 oktober 1997 verschenen eindrapport van de PCCIP stelt onder andere:

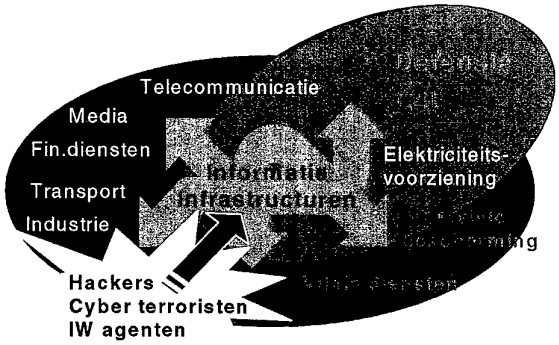
- Een steeds sterker wordende afhankelijkheid van de samenleving van kritische infrastructuren en verhoogde kwetsbaarheid. Veel dreigingen, waaronder: fysieke aanvallen, cyber-dreigingen, systeemcomplexiteit en complexe, onderlinge verwevenheid, blunders, natuurrampen, criminelen, industriële spionage, terrorisme alsmede een gebrek aan bewustzijn.
- De zwakheid van infrastructuren ligt principieel in het gebrekkige begrijpen van onvoorziene gevolgen van de interconnecties voor sturing van (informatie)-infrastructuren (voorbeeld: uit zelfbescherming schakelen elektriciteits-netwerken zich af van buurnetwerken, waardoor een ongewilde cascade optreedt, zie bijv. black-out provincie Utrecht, juni 1997).

Op 10/03/1997 brak een jeugdige hacker in op een telefooncentrale van Bell Atlantic. Gevolg: de luchtverkeersleiding van het Worchester vliegveld nabij Boston had gedurende 6.5 uur geen telefoon- en dataverbindingen meer. Ook kon de verlichting van de landingsbanen niet meer aangezet worden.
Een andere hacker onderbrak de 911-service in Florida voor enige tijd.
(Overigens is de 911 software al lang in het bezit van de hackersgemeenschap.)

- De nationale defensie betreft niet alleen de overheid meer; economische veiligheid heeft niet alleen meer van doen met bedrijven: er is een nieuwe vorm van defensieve samenwerking tussen overheid en de private sector nodig.
- Aanbevolen wordt om:
  - breed de bewustwording te verhogen en de opleiding te verbeteren,
  - middels "best practices" programma's snel een aantal beveiligingsdrempels fors te verhogen, waaronder het uitvoeren van afhankelijkheids- en kwetsbaarheid-analyses,
  - isolatie van kritische infrastructuren van openbare infrastructuren, eventueel met veilige firewalls,
  - het overheids-R&D budget voor IW-InfoSec ineens te verdubbelen tot M$ 500 en daarna jaarlijks met M$ 100 te verhogen tot 2004,
  - wetgeving aan te passen om een gezamenlijke (overheid, publieke sector en bedrijven) aanpak van dreigingen en dreigingsanalyse te kunnen uitvoeren.

Op 18 april 1998 ging een groot deel van het AT&T frame relay netwerk een gehele dag plat ten gevolge van een softwarefout in de gebruikte Stratacom frame relay routers. Ruim 6600 bedrijven verloren hun IT-connectiviteit.

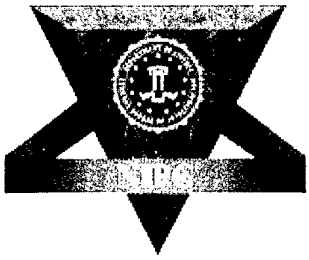
Als uitvloeisel van het PCCIP rapport zijn door President Clinton op 22 mei 1998 twee presidentiële directieven getekend (PDD 62 en PDD 63). PDD 62 behandelt "combatting terrorism". Directive PDD 63 richt zich op de bescherming van kritische infrastructuren. Voor iedere kritische infrastructuur of sector is een verantwoordelijke dienst aangewezen. In 2003 moeten de infrastructuren beschermd zijn tegen aanvallen. In 2000 moeten de Amerikaanse overheids-systemen al veel beter beschermd zijn tegen aanvallen dan nu het geval is.
De coördinatie ligt bij de National Coordinator die ondersteund wordt door het nieuwe Critical Information Assurance Office (CIAO), waarin vrijwel alle kritische departementen en services vertegenwoordigd zijn.[21] Het CIAO onderhoudt nauwe relaties met het National Infrastructure Protection Center (NIPC) (zie volgende paragraaf).




*Figuur 5.1: Wat staat er op het spel?*

[21] Zie: http://www.ciao.org

### 5.7.3.3 USA: National Infrastructure Protection Center (NIPC)




Als uitwerking van de aanbevelingen van de PCCIP commissie is begin maart 1998 het National Infrastructure Protection Center (NIPC) opgericht. Dit is een samenwerkingsverband van de FBI, DOD, USSS, Department of Energy, Department of Transportation, de inlichtingendiensten en de private sector. De grootste inbreng qua kennis en ervaring wordt geleverd door het Computer Investigation and Infrastructure Threat Assessment Center (CITAC) van de FBI dat in het NIPC opgegaan is. Doel is het als een soort "early warning center" uitvoeren van real-time monitoring en detectie van hacker aanvallen op de US nationale elektronische infrastructuren. In 1999 wordt daarvoor M$ 64 uitgetrokken. Het NIPC omvat 85 FBI agenten en 40 medewerkers van andere agencies en de industrie. Zeven teams, tezamen 75 man, worden gestationeerd in Chicago, New York, Dallas, Boston, Los Angeles en Washington DC. [Sign0798]. Het geheel staat onder leiding van Michael A. Vatis, die veel in de publiciteit treedt om het NIPC 'te verkopen' [Cyb98]. Hierbij wordt de ernst van incidenten wel eens 'opgeklopt'.

De missie van het NIPC:

- Het detecteren, evalueren en onderzoeken van aanvallen op de kristische infrastructuren, het reageren hierop en het uitbrengen van waarschuwingen.
- Het coördineren van computerinbraak onderzoeken.
- Het bieden van volledig ondersteuning bij opsporingen ten behoeve van justitie, tegen terrorisme en tegen buitenlandse verzamelaars van inlichtingen.

Onderdeel van hetzelfde initiatief is de oprichting van het Defense Computer Forensic Center (DCFC). Dit moet het basismateriaal verzamelen voor het ministerie van Justitie, die verantwoordelijk is voor de vervolging. Daarnaast heeft het Department of Defense een eigen DoD Critical Infrastructure Protection Integration programma opgestart. Hieronder vallen de bescherming van 'critical assets' (CAAP), infrastructuren (IAP) en een defensie-breed informatie-beschermingsprogramma (DIAP) [InfoW98; sessie P6].

Het is de vraag of de deelname van de private sector binnen het NIPC zal lukken. Er is veel wantrouwen te beluisteren. Ten eerste geeft de private sector informatie uit handen aan de FBI. Er is geen of nauwelijks terugkoppeling van informatie, het lijkt eerder op eenrichtingsverkeer. Daarnaast is de private sector huiverig om informatie uit handen te geven die kan leiden tot enige wettelijke aansprakelijkheid en zijn de risico's dat vertrouwelijk gegeven informatie ongewild uitlekt niet uitgesloten. Het ontbreekt hierbij aan wettelijke kaders die de anonieme informatie-uitwisseling over "cyber attacks", "inbraken", "verkenningen" en dergelijke door de gehele private sector stimuleren.[22] Ook wordt door de private sector het risico van vervolging op grond van de anti-trust wetgeving als aanwezig geacht.

---

22 Vanuit de industrie, maar ook vanuit de FBI en de technische commissie van de Senaat werd tijdens de InfowarCon'98 conferentie aangegeven dat een wettelijke bescherming van bronnen vereist is om het NIPC streven waar te kunnen maken.

Inmiddels heeft het Banking Industry Technology Secretariat (BITS) wel een samenwerking gestart met het NIPC[23].

Opvallend dat de dreigingen waartegen het NIPC opereert "wereldwijd" zijn, maar dat de kritische infrastructuren blijkbaar aan de grens van de Verenigde Statenten stoppen. Het NIPC heeft geen "outreach" of wederzijdse uitwisseling met andere landen in haar plannen opgenomen.

### 5.7.4 USA: IW-HackInt ontwikkelingen (GAO)

De Amerikaanse rekenkamer (GAO) [GAO96] rapporteerde in mei 1996 over pogingen van hackers om (US) Defensiesystemen binnen te dringen. Conclusie: er is een probleem. Tegelijkertijd zijn er zo'n 120 landen die bedreigende kennis van hacking-technieken en mogelijkheden voor hackint hebben.
In één jaar zijn er volgens de schattingen van de GAO 250.000 hack-pogingen, waarvan 2/3 (kunnen) leiden tot het doorbreken van enige vorm van beveiliging ('succes'). Uit eigen testen blijkt dat detectie slechts in 4% van de gevallen plaatsvindt. Slechts één op de 150 pogingen die wordt gedetecteerd, wordt ook gerapporteerd.
Een voorbeeld:

- De inbraak in 1994 op systemen van Rome Labs betekende een verliespost van 1 miljoen gulden. Pas na 5 dagen werd ontdekt dat 2 hackers 7 systemen volledig overnamen. Tevens waren 23 andere systemen gecompromitteerd. De hackers bleken in de UK te zitten en wisten daar ook gratis gebruik te maken van de telefoon. De hackers probeerden onder andere ook binnen te komen bij NASA, NATO en STC.

Aanbevelingen:

- Verbeter het beveiligingsbeleid en -procedures;
- Verhoog het beveiligingsbewustzijn en de controle;
- Er dient een minimale standaard voor opleiding en voor tijd voor beveiligingstaken te worden bepaald;
- Pro-actieve beveiligingsmechanismen dienen ontwikkeld en ingevoerd te worden;
- Defensie dient een effectief antwoord op beveiligingsincidenten te hebben (ook offensief de hacker te lijf gaan!).
- Verplicht rapportage over incidenten aan bevoegd gezag.

Geconcludeerd wordt dat informatiebeveiliging uitermate belangrijk wordt, doch achterblijft bij de groeiende kwetsbaarheden. Dit terwijl defensie en de individuele "krijger" steeds afhankelijker wordt van juiste informatie in diezelfde systemen en netwerken.
Defensieprojecten proberen te komen tot automatische detectie en analyse van inbreuken (intrusion detection), bijv. Automated Security Incident Measurement (ASIM), DARPA's LSS researchprojecten.

---

23 CNET news, 21 Mei 1999 "Big banks move on Net security"

In september 1998 heeft de GAO een nieuw rapport uitgebracht betreffende audits van overheidssystemen die tussen maart 1996 en augustus 1998 hebben plaatsgevonden [GAO98-92]. Het gemis aan beveiligingsbeleid, beveiligingsmanagement en adequate risiso-management wordt aan de kaak gesteld. Bij de onderzochte 24 overheidsorganisaties werden er op een enkele uitzondering na, serieuze zwakheden in de beveiliging onderkend m.b.t. de aspecten beleid en management, toegangscontrole, applicatieontwikkeling en change management, scheiding van verantwoordelijkheden, systeemsoftware instellingen en beschikbaarheid van de dienst. In mei 1999 is een vergelijkbaar vernietigend rapport uitgebracht over de beveiligingssituatie van operationele NASA systemen.

### 5.7.5 USA: IW-Infra & Hackint

#### 5.7.5.1 Oefening Eligible Receiver'97

Tussen 9 en 13 juni 1997 werd door de Amerikanen een Info Ops oefening gehouden onder de naam Eligible Receiver 97. Deze oefening bestond uit twee delen:

- Gesimuleerde aanvallen op de civiele nationale infrastructuur (NII). Zo werd onder andere via een Email-aanval het 911-systeem overbelast. Een ander doel was de energievoorziening. De conclusie was dat de gesimuleerde aanvallen grote kans van slagen hadden om de civiele infrastructuren op zijn minst tijdelijk ernstig te storen.
- Werkelijk indringpogingen in militaire netwerken. Na drie maanden verkenning en voorbereiding met behulp van probing en het plaatsen van uit het public-domain verkregen sniffers en Trojaanse paarden, gingen 20 teams bestaande uit een IW-aanvaller en een waarnemer aan de slag conform een eerder vastgesteld draaiboek. Zodra 'root'-permissie was verkregen, werd een markeringsfile voor de systeembeheerder achtergelaten als bewijs van overname. Opvallend was dat slechts 30% van deze markeringen gedetecteerd werden door de systeembeheerders.

Eligible Receiver 97 had tot doel na te gaan of tegenstanders de mogelijkheid hebben om het US beleid te wijzigen, hun eigen identiteit te verbergen en een militair antwoord daarop te verhinderen of te vertragen. Geconcludeerd is dat militaire systemen en infrastructuren kwetsbaar zijn. De oefening toonde aan dat tussen de 62% en 65% van de overheidsinformatiesystemen gaten bevatten, die uitgebuit kunnen worden door aanvallers. Een aantal systemen kon eenvoudig overgenomen worden. Daarnaast worden pogingen tot indringing tijdens de verkenning in het geheel niet gedetecteerd (slechts 2 keer van de 41.500 bezochte systemen).
Impliciet kan ook geconcludeerd worden dat de Verenigde Staten nu capaciteiten in huis hebben om offensieve IW toe te passen.

#### 5.7.5.2 USA: Infrastructure protection

Zowel in NATO-verband als bilateraal proberen de Verenigde Staten de bondgenoten ervan te overtuigen dat Information Operations en aandacht voor infrastructuurbescherming een harde en urgente noodzaak is. De US deputy secretary of Defense, Dr. John.J. Hamre heeft daartoe in mei en juli 1998 een aantal Europese landen en het NATO hoofdkwartier bezocht. In zijn briefings, ook voor ons Ministerie van Defensie (en genodigden), worden onder andere de uitkomsten van Eligble Receiver uit de doeken gedaan en probeert hij andere landen te bewegen om zich ook met infrastructuurbescherming bezig te gaan houden. [Hamre]

### 5.7.6 USA: civiele Hackint kwetsbaarheden

Er zijn een groot aantal indicaties van kwetsbaarheden van civiele systemen en infrastructuren:

- Het tiger team van IBM gaat op verzoek van klanten na wat de kwetsbaarheid van hun netwerk is. In 90% van zo'n 300 keer wist men binnen 30 minuten succesvol in te breken.
- Een studie van Dan Farmer eind 1996 bleek eenderde van de onderzochte gevoelige websites binnen luttele seconden open te breken te zijn en nog eens eenderde bleek met enige kennis van hacking open te breken te zijn (hhtp://www.trouble.org).

### 5.7.7 USA: Info Ops R&D

Het US Defence Advanced Research Projects Agency (DARPA), Information Technology Office (DARPA/ITO)[24] heeft een aantal programma's lopen om de kwetsbaarheid van systemen, vooral tegen IW-InfoSec aanvallen te verminderen [darpaito]. De term informatiebescherming ("Information Assurance") komt sinds eind 1997 sterk naar voren als alternatief voor de te sterke militair nadruk op "Warfare" in IW-Defensive.

Hierbij wordt uitgegaan van de volgende researchconcepten:

- terugval op "veilige havens" indien systemen en netwerken aangevallen worden;
- tactische waarschuwing en aanvalsanalyse (TW/AA) bij een IW-HackInt aanval;
- hulpmiddelen om betrappen op "heterdaad" mogelijk te maken in "Cyberspace";
- hulpmiddelen om na te gaan hoe infrastructuren van elkaar afhankelijk zijn (naspeuren MEII).

---

[24] Zie: http://www.darpa.mil/ito

Onder het DARPA research-onderwerpen onderwerp "Survivability of large scale systems (LSS)" vallen projecten als:

- high confidence computing en networking,[25]
- gedistribueerde veilige adaptieve architecturen,
- "snel herstel" strategieën en systemen (overleefbaarheid van netwerk, adaptief beveiligingsbeleid, (ICT)-indringerdetectiesystemen),
- het management van complexe systemen/netwerken,
- de ontwikkeling van veilige software systemen (beveiligingsdozen of wrappers), netwerkpompen en analogie van "biologische" en "dynamische" diversiteit in ICT-systemen en software ter vermindering van kwetsbaarheid (software mutatie, firmware i.p.v. software),
- het concept van een Minimal Essential Information Infrastructure (MEII),
- intrusion detection,
- hack black boxen om achteraf probleemanalyse van beveiligingsincidenten te kunnen uitvoeren.

Doel is het weerstaan van IW-aanvallen op informatie-infrastructuren en op commercial-off-the-shelf (COTS) producten die niet ontworpen zijn om dergelijke aanvallen te weerstaan.

### 5.7.8 USA: Diplomatie en Info Ops

Begin juni 1999 is door het US Center For Strategic & International Studies (CSIS) het rapport "Reinventing Diplomacy in The Information Age" uitgebracht. Opvallend daarin zijn de aanbevelingen om sterk rekening te houden met de wijzigingen die de "Revolution in Information Technology" en "Proliferation of New Media" met zich meebrengen. Diplomatie zal zich opener moeten afspelen en waar effectief gebruik moeten maken van de moderne middelen. PsyOps aspecten spelen een belangrijke rol in de voorziene veranderingen in diplomatie. [CSIS99]

## 5.8 Het Midden Oosten

### 5.8.1 Israël en Egypte

Een analyse door het Jaffee Center voor Strategische Studies, onderdeel van de universiteit van Tel-Aviv, geeft aan dat er verschillende IW ontwikkelingen gaande zijn in het Midden Oosten [InfoW98]. Vooral Israël en Egypte zijn actief op dit gebied, al is er weinig bekend uit open bronnen van de status van de Israëlische IW-ontwikkelingen. Het enige dat genoemd wordt zijn "defensive IW-capabilities".

President Mubarak heeft de Egyptische defensie opdracht gegeven om een IW doctrine te ontwikkelen, zowel defensief als offensief gericht. Bovendien is de Egyptische defensie verantwoordelijk voor de bescherming van de kritische civiele infrastructuren.

---

25 Dit onderzoek loopt bij het US Naval Research Laboratorium (NRL). Via het NATO/RTO/IST panel Information Protection werkgroep (AC/323) is contact gelegd met Carl Landwehr, die dit programma bij het NRL trekt.

### 5.8.2 Iran

Iran ontwikkelt IW capaciteiten als een asymmetrisch antwoord op aanvallen met geavanceerde wapens. Hierbij worden de kwetsbaarheden van de "westerse samenleving" voor infrastructuuraanvallen onderkend.

### 5.8.3 Syrië

Hetzelfde geldt voor Syrië dat zelf nauwelijks kwetsbare informatieinfrastructuren kent.

### 5.8.4 Irak

Voor Irak geldt dat zij lessen getrokken hebben uit de Golfoorlog en inmiddels begrijpen welke kwetsbaarheden er aan infrastructuren kleven. COTS apparatuur en programmatuur is echter nog niet in ruime mate beschikbaar door de VN-sancties.

## 5.9 Azië

### 5.9.1 China

Uitgaande van open Chinese publicaties [China], blijkt dat China zich duidelijk aan het prepareren is op de militaire strategie voor 21e eeuw. Binnen deze strategie neemt Information Warfare een grote rol in.

> "Information-intensified combat methods are like a Chinese boxer with knowledge of vital body points who can bring an opponent to his knees with a minimum of movement" (Chang).

In de belangstelling van China liggen: HPM-wapens; informatiedominantie; informatieafschrikking (strategie); virtual reality voor training, planning en analyse. Onder IW verstaan de Chinezen ook: *computervirus warfare*, *precision strike warfare* (C2W) en *stealth warfare* (publicatie 1995).
Onder IW in beperkte zin onderkent men vijf belangrijke elementen: vernietiging van C2-centra, EW (jamming, anti-radiation), militaire deceptie, operationele geheimhouding, psychologische oorlogsvoering (PSYOPS). Daarnaast wordt het verschil tussen de defensieve en offensieve IW-gebieden apart onderkend. [China]
Uit nog recentere publicaties blijkt dat China Information Operations nastreeft. IW in China: "the aim of information warfare is gradually changing from preserving oneself and wiping out the enemy to preserving oneself and controlling the opponent. Information Warfare includes EW, *tactical deception*, *strategic deterrence*, *propaganda warfare*, PSYOPS, NetWar and *structural sabotage*, all of which have something to do with strategy" [Sig0798]. Opvallend zijn de schuingedrukte aspecten, die niet of nauwelijks in de westerse IW-definities aan bod komen.
Voor de ontwikkeling en het gebruik van Info Ops hebben de Chinezen een afdeling van ruim 1000 medewerkers opgezet [InfoW98, T2].

### 5.9.2 Japan

Er is weinig bekend over de Japanse IW-ontwikkelingen. Wel zijn studies vanuit de Japanse industrie bekend m.b.t. het beschermen van de bedrijven.

### 5.9.3 Singapore

Gegeven de kleine staat en de mogelijke bedreigingen van de informatie-infrastructuren waar Singapore grotendeels van afhankelijk is, heeft de Singaporaanse defensie interesse in IW-ontwikkelingen. Zo werd de InfoWar'98 conferentie door 2 luitenant-kolonels en 2 majoors bijgewoond.

### 5.9.4 Taiwan

Taiwan ontwikkelt naast Electronic Warfare (EW) technologie ook Defensieve Information Warfare (IW-D) technologie voor met name communicatie- en informatie-infrastructuurbeveiliging [Janes 12/11/1997). In mei 1999 is de opzet van een InfoWar R&D task force door de Taiwanese Minister van Defensie aangekondigd in een reactie op de Info Ops mogelijkheden van China.

## 5.10 Verenigd Koninkrijk

### 5.10.1 UK: Militaire domein

Het UK Ministry of Defence (MoD) ontwikkelt momenteel een Defensief IW-beleid. Kernthema's daarvan zijn: *bescherming*, *detectie*, *reactie* en *afschrikken*. Feitelijk een aantal aspecten van de "event cycle" zoals TNO-FEL die gebruikt. Informatie wordt binnen het Verenigd Koninkrijk pas sinds kort als "asset" beschouwd. Ter bescherming van kritische informatie-infrastructuren (bijv. die van ziekenhuizen) stelt de UK MoD voor om wereldwijd te komen tot een "IW-Conventie van Genève".
"Het Verenigd Koninkrijk heeft *geen offensief IW-programma in vredestijd*. Wel worden offensieve technieken toegepast om de defensie (lees: defensieve IW) op orde te krijgen." (Col.Jim Blake, Ass.Dir. Studies, MoD [HSAIW]). Vrij geïnterpreteerd betekent dit dat het Verenigd Koninkrijk in geval van een crisis over offensieve IW-mogelijkheden beschikt en deze probleemloos kan inzetten.

### 5.10.2 UK: Info Ops R&D

Het Defence Evaluation and Research Agency (DERA) te Malvern heeft voor de Engelse overheid een IW-groep van 30 man samengesteld met een omzet van 2.5 miljoen pond. De personeelssamenstelling omvat ook ex-militairen uit "beveiligingsland" en ex-vakmedewerkers van overheidsdisciplines (belasting, telecommunicatie e.d.).
De groep kent de volgende subsecties:

- subsectie *IT-vulnerabilities* met daaronder een IT health check team voor de gehele UK overheid;
- subsectie *System vulnerabilities* (bijv. logistieke keten-analyse) met daaronder Militaire projecten;

- subsectie *IT-Security management.*

Daarnaast wordt samengewerkt met de DERA technologiegroepen: technische menskunde, communicatiekwetsbaarheid, Skynet dreiging, system survivability, IW strategie, air battle management, electronic warfare, RF-wapens, naval IW-dreiging en C2W operational analysis.

### 5.10.3 UK: kwetsbare civiele infrastructuur

Engeland heeft al te maken gehad met infrastructuurbedreigingen door de IRA (IW-Infra). Ook is geconstateerd dat defensie voor een groot deel afhankelijk is van openbare communicatie-infrastructuren welke door circa 160 operators wordt beheerd. DERA verricht daarom onderzoek naar de "Minimum Essential Defence Information Infrastructure" (MEDII).
Ook werkt de Engelse defensie nauw samen met de Amerikanen. DERA heeft geheime samenwerkingsprojecten op dit gebied lopen met Amerikaanse defensie onderzoeksinstellingen.

Het Department of Trade and Industry (DTI) is een nationaal informatie- en infrastructuurbeschermingsprogramma gestart. Voor zover bekend is daar geen vrije informatie over beschikbaar.

## 5.11 Internationale organisaties

### 5.11.1 NATO

NATO kent het Command and Control Warfare (C2W) concept als onderdeel van de landmacht-doctrine. De definitie daarvan is gebaseerd op de Amerikaanse Joint Command IW-definitie. De Nederlandse defensie volgt deze definitie.

Het NATO Civil Communications Planning Committee onderzoekt de veiligheid van publieke telecommunicatiesystemen [NATO96], met name op het gebied van denial-of-service. Onder de bedreigingen worden alleen de militaire (gecoördineerde) bedreigingen als ernstig gerubriceerd. Hackers worden niet als (grote) bedreiging gezien [NATO96, alinea's 16 en 17].

NATO heeft begin 1998 een Info Ops definitie opgesteld, welke geaccepteerd is door de lidstaten [MCM-069-98]. De voorliggende definitie wordt door Nederland en Duitsland als te vaag ervaren en zal voor eigen gebruik van kanttekeningen worden voorzien. In 1998 is door het NATO Military Committee (MC) het Info Ops Policy document opgesteld [MC422], waaraan ook TNO-FEL bijdragen heeft geleverd.

In een lezing voor het Scientific Advisory Forum (SAF) heeft het NC3A in mei 1998 het onderwerp Information Operations aan de orde gesteld. De NC3A Security group werkt aan Information Assurance (netwerk monitors; automatische kwetsbaarheidsanalyse (bijv. ISS) en indringerdetectie). Onderzoek naar

countermeasure-mogelijkheden liggen mogelijk in de belangstelling. Daarvoor moeten natuurlijk eerst de Rules of Engagement (ROE) op politiek niveau worden vastgesteld.

Het NATO RTO panel on Information System Technology (AC/243) zal in oktober 1999 in Washington een NATO symposium over Information Protection houden. Daarnaast is binnen het NATO NC3B/RTO/IST panel een task group die zich bezig houdt met research naar Information Assurance (NetonIP; NATO AC/323). TNO-FEL is daarin vertegenwoordigd.

### 5.11.2 G8 landen

De G8 (Canada, Frankrijk, Duitsland, Italië, Japan, Rusland, het Verenigd Koninkrijk en de Verenigde Staten) hebben op 12 december 1997 de handen ineengeslagen om tezamen te komen tot aanpak van "NetWar" computer-criminaliteit. In het bijzonder is dat gericht op het gebruik van openbare (internationale) netwerken voor (kinder)pornografie, drugstransport en elektronische fraude.
Daartoe worden de volgende acties genomen:

- op elkaar afstemmen en aanpassen van wetten voor de "elektronische snelweg",
- verruiming mogelijkheden voor snelle onderlinge assistentie bij grens-overschrijdende criminaliteit,
- ontwikkelen van hulpmiddelen voor "netzoeking",
- tezamen met de industrie zoeken naar mogelijkheden om high-tech criminaliteit uit te sluiten,
- het verlenen van steun aan internationale organisaties voor standaardisatie om te komen tot betrouwbare datacommunicatie en beveiligde systemen (InfoSec en CompuSec).

### 5.11.3 Europol

Europol richt zich met name op de bescherming tegen computercriminaliteit. De Europol wetgeving staat Europol een aantal vrijheden toe. De mogelijkheid om te opereren vanuit een Europees land met de meest 'flexibele' wetgeving op de elektronische snelweg wordt als operationele optie onderkend.[26]

26 Informatie van de heer F. Muhlschlegel van Europol tijdens InfoWar'98.

## 5.12 Nederland

### 5.12.1 NL: Situatieschets defensie

Nederland heeft formeel gesproken nog geen (defensief) Information Operations programma. Wel is er een Krijgsmachtbreed Info Ops overleg (KL, KM, KLu, MID, DS, CIS en TNO). Daarnaast is de belangstelling voor het onderwerp Information Operations binnen en buiten Defensie snel groeiende. Enkele indicaties:

- Defensie
  - Belangstelling bij de KMA voor IW uit oogpunt van militaire ontwikkelingen.
  - Tijdens het symposium "IT in de Krijgsmacht", oktober 1996, gaf minister Voorhoeve aan dat IT een tweesnijdend zwaard is, waarbij vijandige staten, criminelen en anderen betrekkelijk eenvoudig ("David en Goliath") inbreuk maken op de IT-voorziening. Bovendien wordt "cyberwar" als dreiging voor de westerse voorsprong op militair gebied gezien. Na de constatering dat IT ook defensief gebruikt moet worden, werd het onderwerp losgelaten. Kol. Oude Lohuis ging in zijn lezing over Force XXI wel dieper in op IW en stelt dat Defensie over een toonaangevend expertisecentrum op IT-beveiligingsgebied zou moeten beschikken. Door beiden werd alleen ingegaan op IW-InfoSec. [ITK96]
  - Discussie zoals gevoerd bij het Instituut Defensie Leergangen door Krijgsmachtdelen, Defensiestaf, KMA, KIM en TNO.
  - De oprichting van een NATO Info Ops working group in 1999 binnen het NATO Military Committee, waarin Defensiestaf voor Nederland haar bijdrage/ beleid aan moet dragen.
  - Een Info Ops studie door de Landmachtstaf/BO die medio mei 1998 had moeten resulteren in een rapportage aan de Sous-chef LAS[27].
  - In 1998 leefde bij de KLu de gedachte van de ontwikkeling van een Information Operations cell met een "red team" activiteit.
  - De geplande opzet in 1999 van een Info Ops R&D programma 1999-2003 bij TNO ten behoeve van de Centrale Organisatie van het MinDef.

Enige recente incidenten die onze infrastructuur kwetsbaarheden tonen:
12/3/98: Kabel geraakt bij aanleg tramtunnel centrum Den Haag: uitval gedurende een dag van 900 telefoons van o.a. Min.BiZa en andere ministeries.
22/3/98: Opgegraven glasvezelkabel veroorzaakt uitval van vrijwel alle betaal-automaten in Noord-Nederland.
12/6/98: Gehele dag chaos op Schiphol na uitval Triple A systeem gedurende slechts een half uur.
16/6/99: Het slaan van een damwandplank in Groningen door vier glasvezelkabels leidde tot uitval van vaste en mobiele communicatie in Groningen, Friesland en Drenthe tussen 8 en 19 uur. Gevolgen: uitval van RDW (APK-keuringen, rijbewijzen, auto-overschrijvingen), 1-1-2, politieverbindingen, GSM en interlokaal bellen.

27 Door het vertrek van Maj. E. Witte naar de NATO MC Info Ops groep is de verdere ontwikkeling tijdelijk stilgevallen.

- TNO-FEL's Red team activiteiten in het kader van Information Assurance onderzoeken.

### 5.12.2 NL: Situatieschets civiele bescherming

- Overheid (inclusief Defensie)
  - Vraag om lezingen: BVD [Luiijf98] KMA, Nederlandse Association of Old Crows (AOC), Leergang topmanagement IDL (2 september 1998 en begin 1999), KIVI afdeling Defensieonderzoek, KIM (gegeven door Lkol. Maenen).
  - Kamervragen naar aanleiding uitval regionale meldkamer politie Arnhem en daardoor de overbelasting (en bijna uitval) van de meldkamer Nijmegen en problemen met 1-1-2 via mobiele telefoons, met name bij uitval/ overbelasting van de centrale in Zeist en/of de alarmcentrale van de KLPD.
  - Ambtelijke studie door MinEZ naar regelgeving om bij calamiteiten via de publieke operators enige voorrangscapaciteit te kunnen claimen. Nieuwe regelgeving op basis van artikel 14.6 van de Telecomwet regelt continuiteit, toegang en prioriteiten van de Telecominfrastructuren (vast net, het Noodnet en mobiele netwerken) in geval van buitengewone omstandigheden [DGTP99]. Voor GSM geldt [HDTP98] als een voorbeeld.
  - De discussie over de opzet van een studiegroep naar de kwetsbaarheid van (Internet) infrastructuur (DGTP, Stratix, TUDelft, KPN Telecom, TNO). Het wordt voorzien dat deze werkgroep in de tweede helft 1999 zal starten.
- Bedrijfsleven en industrie
  - Rapportages over onvoldoende voorbereiding op calamiteiten door bedrijven (KPMG onderzoek, 9/1997).
  - Reacties naar aanleiding van de langdurige stroomuitval Bleiswijk (1995) en provincie Utrecht (1997).

# 6. IW/ Info Ops: wat is er nieuw?

## 6.1 Militaire domein

De vraag die veel gesteld wordt, is: "Wat is er nieuw aan Information Warfare?". Het antwoord is niet eenduidig te geven. Het gebruik van informatie voor eigen doeleinden, voor defensieve en offensieve doeleinden is al sinds oudsher bewust of onbewust onderdeel van "oorlogsvoering". Zo was honderden jaren geleden het verschijnen van een Mongoolse ruiter op een paardje aan de horizon al reden genoeg om snel een dorp te ontruimen. Informatie over de verschrikkingen waarde sneller rond dan de krijgers zelf!

In de afgelopen decennia is er sluipend een wezenlijke verandering opgetreden in de technologische uitrusting en het optreden van de 'moderne' defensies. Vrijwel alle communicatiemiddelen en informatieverwerking en -verspreiding binnen deze defensies zijn inmiddels gebaseerd op ICT-middelen. Tegelijkertijd is de wijze van optreden verschoven van "slagveld" naar "bijna chirurgische precisie" en "joint" aanpak. Dit vergt nauwkeurige afstemming over de gesynchroniseerde aanpak van geselecteerde doelen met geschikte middelen en vereist dat correcte informatie over eigen middelen en intelligence over de doelen voor allen beschikbaar is. Omdat informatie een veel essentiëlere 'productiefactor' geworden is dan vroeger, is de integriteit en beschikbaarheid van de informatieinfrastructuur van uitermate groot belang tijdens alle vormen van optreden (uiteenlopend van consultatie bij peacekeeping tot doelaanwijzing tijdens operationeel optreden).

Nieuw is het inzicht dat gecombineerd en uitputtender gebruik van reeds bestaande middelen plus het ontzeggen van de tegenstander van het gebruik van dergelijke middelen, escalatie van conflicten kan verminderen zo niet kan voorkomen. Onder deze middelen vallen onder andere: "all source intelligence", informatiedistributie, inzet van ICT voor psychologische beïnvloeding.

Het strategisch - operationeel gebruik van informatie en informatiemiddelen binnen wat Information Operations heet is dan ook een logische, evolutionaire ontwikkeling van "oude" principes. Het "nieuwe" is dat de technologische ontwikkeling nu de mogelijkheden geeft om de combinatie van oude middelen en nieuwe ICT-middelen effectief als bepalende factor in te zetten.
Dit vergt aanpassing van strategie en de wijze waarop nieuwe, op ICT gebaseerde militaire technologie ingezet wordt.

## 6.2 Civiele domein

Aan de civiele kant zijn de 'moderne' landen in de afgelopen decennia ook sluipend veel afhankelijker geworden van de infrastructuren. Omdat het vrijwel altijd goed gaat, is er weinig aandacht besteed aan risicospreiding en risicobeheersing. Zo ontdekte onze westerse samenleving tijdens de oliecrisis begin jaren zeventig dat vrijwel al ons transport afhankelijk is van een ongestoorde oliebevoorrading.
De steeds verdergaande koppelingen tussen informatie- en andere infrastructuren (bijv. glasvezels in spoordijken; beheer/controle op afstand van onderstations via telefoonlijnen, zonder elektriciteit werkt de verwarming niet en kunnen we niet meer afrekenen) en de globalisering daarvan, maakt onze samenleving kwetsbaar voor grootschalige onderbreking veroorzaakt door bijvoorbeeld natuurgeweld of activisten. Langzamerhand ontstaat het inzicht dat deze kwetsbaarheden en afhankelijkheden beheerst moeten worden om ernstige verstoring van onze samenlevingen uit te sluiten.

Ook hier is niet sprake van een sprongsgewijs "nieuw", maar van een sluipende wijziging in "oude, bekende" kwetsbaarheden. Door de groeiende complexiteit van (informatie)infrastructuren en hun onderlinge afhankelijkheden en ook de afhankelijkheid van onze samenleving van die infrastructuren, is de kwetsbaarheid van onze samenleving inmiddels sterk verhoogd. Een dergelijke achilleshiel geeft activisten en landen die ons willen treffen een doel in handen.

Onze nationale veiligheid kan niet meer alleen gewaarborgd worden door onze defensie. We zijn sterk afhankelijk van globale infrastructuren, welke niet meer onder overheidscontrole vallen. Bescherming daarvan vergt coöperatie van meer landen en van civiele, multi-nationale en internationale organisaties.

Ook onze defensie is sterk afhankelijk van de infrastructuren binnen onze samenleving. Deze zijn inmiddels van buiten af, zonder noodzakelijke fysieke toegang tot ons land, te verstoren. Ook richten activisten/terroristen zich steeds meer op civiele doelen dan op militaire doelen.
Bescherming van infrastructuren in het civiele domein is daardoor noodzakelijk om ook in het militaire domein vrijheid van consultatie, beslissen en acteren te waarborgen.

## 6.3 Bilaterale NL-DU Information Operations studie

Begin 1998 heeft Defensie met het Duitse Bundesministerium der Verteitigung afgesproken om een gezamenlijke, bilaterale studie "Information Operations" uit te voeren. De leiding ligt aan Nederlandse zijde bij Defensiestaf, afd. Conceptuele Zaken. TNO-FEL en KMA nemen deel aan deze studie (project 015.28160/28853). Aan Duitse zijde neemt het Amt für Studien und Übungen der BundesWehr deel. Dit Amt heeft begin oktober 1998 het IABG ingehuurd om hen te helpen bij deze

studie. Het Max Planck instituut in Heidelberg heeft input geleverd voor de (inter)nationale juridische aspecten.

Onderdeel van het NL-DU bilaterale Information Operations project vormt een gezamenlijke presentatie medio 1999 over Information Operations in beide landen.

De uitkomsten van deze studie zullen een raamwerk voor Information Operations opleveren zoals Nederland en Duitsland dat zien. Uitgaande van dit raamwerk kunnen de Info Ops speerpunten qua op te lossen problemen en qua nodige ondersteuning binnen Defensie geïdentificeerd worden. Aan TNO-Defensie-onderzoek (FEL en TM) is het om de Nederlandse Info Ops koers en de aanbevelingen naar de Krijgsmachtdelen toe te vertalen in het Info Ops R&D programma 2000-2003.

# 7. TNO en Info Ops / Information Assurance

TNO heeft de pretentie het Nederlandse "Center of Excellence" te zijn op het gebied van infrastructuurbescherming, Information Assurance onderzoek en Information Operations R&D:

Daartoe wordt in 1999 een Info Ops researchprogramma opgezet in overleg met de Centrale Organisatie van het Ministerie van Defensie. Strategische relaties op dit gebied met buitenlandse collega R&D instellingen zullen in 1999 onder auspiciën van Defensie tot stand gebracht worden.
Leidend hierbij zijn de resultaten en aanbevelingen van de bilaterale NL-DU studie Info Ops.

TNO staat open om de Nederlandse overheid ter zijde te staan bij de bescherming van de overheid en kritische infrastructuur tegen Info Ops dreigingen.

# 8. Literatuur

## 8.1 Historische Information Warfare literatuur

[Arquil] Cyberwar is coming; Jon Arquilla en David Ronfelt, 1993

[Jens94] Information Warfare: Principles of Third-Wave War; Owen Jensen. Airpower Journal (winer 1994); 35-43

[Lib] What is information Warfare?; Martin Libicki, Nationale defense University, Institute for National Strategic Studies. http://www.ndu.edu/ndu/inss/actpubs/act003/a003.html

[Magsig] Information Warfare in the Information Age; Daniel E. Magsig

[Stein] Information Warfare; Prof George J. Stein

[WSchw] Information Warfare, Chaos on the electronic superhighway; Schwartau,Winn, 1994

[Toffler] The Third Wave, 1980, Powershift, 1990 en War and Anti-war: Survival at the Dawn of the 21st Century, door Alvin and Heidi Toffler, 1993

## 8.2 Information Warfare

[Bosch97a] Generaals, geleerden en goeroes: kanttekeningen bij oorlog, informatie en informatie-oorlog, april 1997, Bgen. Prof. J.M.J. Bosch

[Bosch97b] 'Information Warfare', een verkenning; 19/11/1997, Bgen. Prof. J.M.J. Bosch

[China] The Challenge of Information Warfare, Major General Wang Pufeng; Information Warfare, Senior Colonel Wang baocum Li Fei; Information War: A New Form of People's War, Wei Jincheng (http://198.80.36/91/ndu/books/chinview/ )

[Dbund] Bundeshaus persmededeling 13/05/1996, nummer 405-96.

[DSB96] Report of the Defense Science Board Task Force on Information Warfare - Defense (IW-D), US Defense Science Board, November 1996, (http://jya.com/iwdmain.html)

[DWT97] Chancen und Risiken des Factors Information - Auswirkungen auf Pilitik, Gesellschaft, Wirtschaft und Militär, 19. und 20. November 1997, Deutschen Studiengesellschaft für Wehrtechnik mbH (FEL bibliotheeknr. ER98-01)

[GAO96] Information Security: Computer Attacks at Department of Defense Pose Increasing Risks, GAO Executive report B-266140, 22 mei 1996 (http://www.infowar.com/CIVIL_DE/gaosum.html-ssi of http://www.gao.gov).

[GAO98-257] Defense Information Superiority: Progresses Made, but Signicant Challenges Remain, GAO/NSIAD/AIMD-98-257, Augustus 1998, (http://www.gao.gov).

[HSAEW] Information Warfare, Mr. E. Waltz, H.Silver and Associates, June 1997

[HSAIWC] Information Warfare conference proceedings, H.Silver and Associates, Londen, 13&14 November 1997

[InfoW98] InfoWar'98 conference proceedings, sept.1998

[Potom98] Seminar on Cyber-Terrorism and Information-Warfare: Threats and Responses, Proceedings report PIPS-98-2, 16 April 1998, Potomac Institute for Policy Studies, Arlington, VA, USA

[Rand96] Survivability Architectures, Rand, 6/1996, http://www.cs.virginia.edu/~survive

## 8.3 Information Operations

[FM 100-6] Information Operations, US Army, 27/8/1996 http://www.jya.com/fm100/fm100-6.htm)

[JP3-13] Joint Pub 3-13, 'Joint Doctrine for Information Operations', Joint Chiefs of Staff, 9 October 1998 via http://www.dtic.mil/doctrine/jel/c_pubs2.htm te downloaden

[IDA97] Information Operations: A Research Aid, J.V. Gray et al., IDA, September 1997, IDA document D-2082 (via http://www.infowar.com verkrijgbaar)

[MCM-069-98] [NR] NATO Information Operations (INFO OPS) concept, May 1998

[MC422] NATO Information Operations Policy, 12 January 1999

[NRC99] Realizing the Potential of C4I: Fundamental Challenges. Committee to Review DOD C4I Plans and Programs, National Research Council, May 1999. (http://www.nap.edu/catalog/6457.html)

[Sign0798] Information Operations, AFCEA's Signal, July 1998

## 8.4 Information Peacekeeping

[Steele98] Information Peacekeeping, Robert R. Steele, 1998 htttp://www.oss.net/Info/Peace

## 8.5 Information Security

[JP3-54] Joint Pub 3-54, 'Joint Doctrine for Information Security', Joint Chiefs of Staff, 24 January 1997 via http://www.dtic.mil/doctrine/jel/c_pubs2.htm te downloaden

## 8.6 PSYOPS en CIMIC

[CSIS99] Reinventing Diplomacy in the Information Age, Center for Strategic & International Studies, June, 1999
http://www.csis.org/pubs/diaexecsum.html

[Kleij99] Human Factors in Information Operations. TNO-TM rapport Juni 1999. Kleij, R.van der, Griffioen-Young, H.J., Luiijf, H.A.M., Klaver, M.H.A.

[Wentz98] "Lessons From Bosnia: The IFOR Experience" with PSYOPS, CIMIC, Info Ops, Wentz, L. (ed.)
http://www.dodccrp.org/bostoc.htm

## 8.7 Critical Infrastructure Protection / Information Assurance

[ASDSC] Australia's Vulnerability to Information Attacks; Cobb, Dr. Adam; Australian Strategic and Defence Studies Centre, WP.No. 0301, april 1997, ISBN 07315 27232
http://www.infowar.com/CIVIL_DE/civil_100497a.html-ssi of
http://coombs.anu.edu.au/~acobb/X0016_Australias_Vulnerabi.html

[Cobb98] Thinking of the Unthinkable: Australian Vulnerabilities to High-Tech Risks; Cobb, Dr. Adam; Foreign Affairs, Defece and Trade Group, 29 June 1998, http://www.aph.gov/library/pubs/rp/1997-98/98rp18.htm

[Cyb98] Proceedings report on Seminar on Cyber-Terrorism and Information Warfare: Threats and Responses, Potomac Institute for Policy Studies, PIPS-98-2, 16 April 1998

[HGTP98] Vergunning DCS1800 al dan niet in combinatie met GSM, HGTP/98/594/DCS 135 U, zoals gepubliceerd in de Staatscourant 1998, nr. 45, pg 20.

[DGTP99] Regeling voorbereiding buitengewone omstandigheden Telecommunicatiewet, DGTP/99/914/LF, 7 mei 1999, zoals gepubliceerd in de Staatscourant 1999, nr. 90, pg 8.

[GAO98-92] Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk, September 1998, GAO/AIMD-98-92 (http://www.gao.gov).

[Hamre] Briefing slides en verslag bezoek Dr. Hamre aan MinDef.
Zie daarnaast: http://jya.com/dsd061198.htm

[Luiijf98] Information Assurance and the Information Society. In: Security services in the information society - Assets, cyberattacks and encryption, The Hague, 12-14 May 1998. Seminar Club de Berne, Berne. 1998.
(ongerubriceerde versie is bij de auteur aan te vragen).

[Luiijf99a] Information Assurance and Society. In: Gattiker, U.E., Pedersen, P., and Petersen, K. (Eds.), Conference Proceedings EICAR '99 - European Institute for Computer Anti-Virus Research, Aalborg, Denmark, Feb 27th - March 2nd. EICAR c/o TIM-World ApS,

Aalborg, Denmark. pp. 1-17. ISBN 87-987271-0-9
On-line via http://www.tno.nl/instit/fel/refs

[Luiijf99b] Information Warfare: de kwetsbaarheid van de samenleving. Beveiliging 12(4):52-55. 1999.

[NATO96] [NR] NATO Communications and Information Systems Committee: Overview of Security in Public Telecommunications Systems, AC/317-N/892, June 6, 1996.

[PCCIP] (US) President's Commission on Critical Infrastructure Protection by Executive order #13010 of July 15, 1996. (http://www.pccip.org)

[PCCIPwp] White paper on Critical Infrastructure Protection, mei 1998 http://www.epic.org/security/infowar/cip_white_paper.html

[PDD62] Presidential Directive 1998, number 62 "Combatting Terrorism", 22 mei 1998; (http://www.ciao.gov)

[PDD63] Presidential Directive 1998, number 63 "Critical Infrastructure Protection Directive", 22 mei 1998; (http://www.ciao.gov)

## 8.8 Defensie in de 21ste eeuw

[China] Weapons of the 21st Century, Chang Mengxiong; IW, Senior Colonel Wang Baocun and Lei Fi and more (http://198.80.36.91/ndu/inss/books/chinview/chinapt4.html)

[JV2010] Joint Vision 2010, USA, (http://www.dtic.mil/)

[NWVista] New World Vistas: Air and Space Power for the 21st Century Air Force Study, 1995

## 8.9 Overige World Wide Web bronnen

[darpaito] DARPA/ITO pagina's over survivability van large scale systems (LSS), (http://www.ito.darpa.mil/ResearchAreas/LSS.html en WC.html)

[tnoiwdef] Information Operations en Information Assurance webpagina's TNO-FEL: http://www.tno.nl/instit/fel/infoops

[tnoinfsec] InfoSec webpagina TNO-FEL: http://www.tno.nl/instit/fel/infosec

[Tradoc] http://www-tradoc.army.mil/dcscd/spaceweb (/informat.htm)

## 8.10 Overige referenties

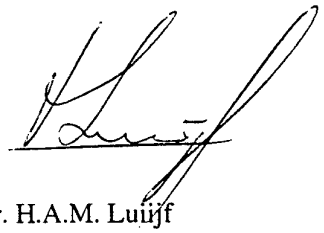
[ITK96] Symposiumbundel "IT in de Krijgsmacht, op weg naar de 21e eeuw", 30 oktober 1996, KMA en Vereniging Officieren Informatica

[Nolan] Nolan, R.L. and Gibson, C. (1974), 'Managing the four stages of EDP Growth', Harvard Business Review, 1974(2) pp 76-88
en Nolan, R.L. (1979). 'Managing the crises in data processing', Harvard Business Review, 1979(3/4) pp 115-126

# 9. Index

# 10. Ondertekening

Dr. L. Smit
Groepsleider



Ir. H.A.M. Luijf
Auteur

# Bijlage A Lijst van afkortingen

| | |
|---|---|
| ACE | Analysis Control Element |
| ANSIR | Awareness of National Security Issues and Response |
| ASDSC | (AUS) Australian Strategic and Defence Studies Centre |
| ASIM | Automated Security Incident Measurement |
| BITS | Banking Industry Technology Secretariat |
| BZK | (Ministerie van) Binnenlandse Zaken en Koninkrijksrelaties |
| CA | Civil Affairs |
| CAAP | (US DoD) Critical Asset Assurance Program |
| CERT | Computer Emergency Response Team |
| CCD | Camouflage, Concealment, and Deception |
| CCM | Communication Counter Measures |
| CFEWC | Canadian Forces EW Center |
| CFIOG | Canadian Forces Information Operations Group |
| CFIPC | Canadian Forces Information Protection Center |
| CIAO | (US) Critical Infrastructure Assurance Officer |
| CICG | (US) Critical Infrastructure Coordination Group |
| CIMIC | (NATO) Civil-Military Co-operation |
| CIP | Critical Infrastructure Protection |
| CIPU | Critical Infrastructure Protection Unit |
| CIS | Communications and Information System |
| CITAC | (FBI) Computer Investigation and Infrastructure Threat Assessment Center |
| CNA | (NATO) Computer Network Attack |
| CND | (NATO) Computer Network Defence |
| COMINT | Communications Intelligence |
| COMPUSEC | Computer systems security |
| COMSAT | Communications satellite |
| ComSec | Communications Security |
| COTS | Commercial off-the-shelf |
| CYW | Cyber(netic) Warfare |
| C2 | Command and Control |
| C2CS | (NATO) Command and Control Communication System |
| C2IS | (NATO) Command and Control Information System |
| C2W | Command and Control Warfare |
| C3 (1) | Command, Control and Communications |
| C3 (2) | (NATO) Consultation, Command and Control |
| C3CM | Command, Control and Communications countermeasures |
| C3I | Command, Control, Communications and Intelligence |
| C3ISR | Integrated Control, Communications, Intelligence Surveillance and Reconnaissance |
| C4D | Chaos, Catastrophy, Confusion, Computers and Deception |
| C4I | Command and Control, Communications, Computers and Intelligence |
| C4ISR | Command and Control, Communications, Computer Intelligence, Surveillance and Reconnaissance |
| DARPA | (US DoD) Defense Advanced Research Projects Agency |
| DASD | Deputy Assistant Secretary Department |
| DBS | Digital Broadcasting System |
| DCFC | Defense Computer Forensic Center |
| DERA | (UK) Defence Evaluation and Research Agency |
| DEW | Directed Energy Weapons |
| DIA | (US DoD) Defense Intelligence Agency |
| DIAP | (US DoD) Defense-wide Information Assurance Program |
| DII | Defence Information Infrastructure |
| DISA | (US DoD) Defense Information Systems Agency |
| DoD | (US) Department of Defense |

| | |
|---|---|
| DoDD | (US) Department of Defense Directive |
| DOS | Denial-of-Service |
| DSB | (US) Defense Science Board |
| EA | EW - Electronic Attack |
| EC | Electronic Combat |
| ECCM | Electronic Counter-Counter Measures |
| ECM | Electronic Counter Measures |
| EFT | Electronic Funds Transfer |
| EEI | Essential Elements of Information |
| EIW | Economical Information Warfare |
| ELINT | Electronic Intelligence |
| EM | Emergency Management |
| EMCON | EMissions CONtrol |
| EMP | Electronic Magnetic Pulse |
| EO/IRCM | Electro-optical/Infrared Counter Measures |
| EOV | Elektronische Oorlogvoering (= EW) |
| EP | EW - Electronic Protection |
| EPM | EW - Electronic Protection Measures |
| ES | EW - Electronic Support |
| ES | Electronic warfare Support |
| ESM | Electronic (warfare) Support Measures |
| EW | Electronic Warfare (=EOV) |
| EZ | Ministerie van Economische Zaken |
| FEL | TNO Fysisch en Elektronisch Laboratorium |
| FEMA | (US) Federal Emergency Management Agency |
| FISINT | Foreign Instrumentation Signals INTelligence |
| G-2 | Army or Marine Corps component intelligence staff officer or section |
| GAO | (US) Government Accounting Office ('Rekenkamer') |
| GCCS | (US DoD) Global Command and Control System |
| GII | Global Information Infrastructure |
| GPS | Global Positioning System |
| GSM | Global System for Mobile Communications |
| HackInt | Hackers Intelligence |
| HERF | High Energy Radio Frequency |
| HPM | High Power Microwaves |
| HUMINT | Human Intelligence |
| InfoSec | Information Security (informatiebeveiliging) |
| IA | Information Assurance |
| IATF | Information Assurance Task Force |
| IABG | Industrieanlagen-Betriebsgesellschaft mit beschrankter Haftung |
| IAP | (US DoD) Infrastructure Assurance Program |
| IBDA | Information Battle Damage Assesment |
| IBW | Intelligence-based Warfare |
| ICT | Information and Communication Technology |
| ID | Information Dominance |
| IITF | (US) Information Infrastructure Task Force |
| ILS | Instrument Landing System |
| IMINT | Imagery Intelligence |
| Info Ops | Information Operations |
| IO | Information Operations (old abbreviation - abandoned because of conflict with International Organization) |
| INFOSEC | information systems security |
| IPB | Intelligence Preparation of the Battlespace |
| IPTF | (US) Infrastructure Protection Task Force |
| IRT | Incident Response Team |
| ISAC | (US) Information Sharing and Analysis Center |
| ISDN | Integrated Services Digital Network |
| IW | Information Warfare |

| | |
|---|---|
| IW-C2W | Information Warfare deelgebied Command and Control Warfare |
| IW-D | Defensive Information Warfare<br>ook wel: Information Warfare-Defense (oudere term) |
| IW-EM | Information Warfare deelgebied Emergency Management |
| IW-EW | Information Warfare deelgebied Electronic Warfare |
| IW-Infra | Information Warfare deelgebied Infrastructure Warfare |
| IW-O | Information Warfare–Offense |
| IST | Information Systems Terrorism |
| IT | Information Technology |
| J-2 | Intelligence Directorate of a joint staff |
| J-3 | Operations Directorate of a joint staff |
| J-6 | C4 Systems Directorate of a joint staff |
| JIC | Joint Intelligence Center |
| JTF | Joint Task Force |
| JV 2010 | Joint Vision 2010 (US DoD Publication) |
| KIM | Koninklijk Instituut voor de Marine |
| KMA | Koninklijke Militaire Academie |
| KLPD | Korps Landelijke PolitieDiensten |
| KLu | Koninklijke Luchtmacht |
| KMA | Koninklijke Militaire Academie |
| LSS | Survivability of large scale systems (DARPA/ITO programma) |
| MAD | Mutual Assured Destruction |
| MASINT | Measurement and Signatures Intelligence |
| MEDII | Minimum Esssential Defence Information Infrastructure |
| MEII | Minimum Essential Information Infrastructure |
| MEF | Marine Expeditionary Force |
| MID | Militaire Inlichtingendienst |
| MIE | Military Information Element |
| MISSI | (US) Multilevel Information Systems Security Initiative |
| MoD | Ministry of Defence |
| MT | Management Team |
| NASA | National Aeronautics and Space Administration |
| NATO | North Atlantic Treaty Organisation |
| NVAT | (CAN) Network Vulnerability Assessment Team |
| NDU | (US) National Defense University |
| NII | National Information Infrastructure (US en Australië) |
| NIPC | (US) National Infrastructure Protection Center |
| NNEMP | Non-nuclear Electronic Magnetic Pulse |
| NRIC | (US) Network Reliability and Interoperability Council |
| NRO | (US) National Reconnaissance Office |
| NSA | (US) National Security Agency |
| NSTAC | (US) National Security Telecommunications Advisory Committee |
| OASD | Organization of the Assistant Secretary of Defense |
| OODA | Observation-Orientation-Decision-Action |
| OPSEC | Operations Security |
| OSCINT | Open Source Intelligence |
| PBX | Telefooncentrale |
| PCCIP | (US) President's Commission on Critical Infrastructure Protection |
| POTS | Plain Old Telephone System |
| PSO | Peace Support Operations (NATO) |
| PSPA | Peace Support Phychological Activities (NATO) |
| PSTN | Public Switched Telephone Network |
| PSYOPS | Psychological (Warfare) Operations |
| PSYW | Psychological Warfare |
| RADINT | Radar Intelligence |
| RII | Relevant Information and Intelligence (Info Ops component) |
| RMA | Revolution in Military Affairs |
| RMP | Risk Management Program |

| | |
|---|---|
| ROE | Rules of Engagement |
| S2 | Battalion or brigade intelligence staff officer or section |
| SCADA | Supervisory Control and Data Acquisition (energy distribution) |
| SIGINT | Signals Intelligence (ELINT en COMINT) |
| STC | Shape Technical Centre |
| TELINT | Telecommunications Intelligence |
| TIW | Transnational Infrastructure Warfare |
| TW/AA | Technical warning/Attack assessment |
| TNO | Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek |
| TNO-FEL | TNO Fysisch en Elektronisch Laboratorium |
| TNO-STB | TNO Strategie, Technologie en Beleid |
| TNO-TM | TNO Technische Menskunde |
| WMD | Weapons of Mass Destruction |
| WRR | Wetenschappelijke Raad voor het Regeringsbeleid |

# Bijlage B Een wereld aan IW-definities

Om te proberen inzicht te verkrijgen in Information Warfare is gezocht naar definities. Navolgend zijn een aantal van de definities weergegeven.

## B.1 Information Warfare definities, niet-land gebonden

**Thomas Rona [Lib]:**

The strategic, operation, and tactical level competitions across the spectrum of peace, crisis, crisis escalation, conflict, war, war termination, and reconstitution/restoration, waged between competitors, adversaries or enemies using information means to achieve their objectives.

**Working definition US National Defense University (R.Neilson and C.B. Giasson, 1995):**

Information Warfare is an approach to conflict focusing on the management and use of information in all its forms and at all levels to achieve a decisive advantage in pursuit of national security goals.
Information based warfare is both offensive and defensive in nature - ranging from measures to prohibit adversaries from exploiting information to corresponding measures to ensure the integrity, availability and interoperability of friendly information assets.
Information based warfare is also waged in political, economic and social arenas and it is applicable over the entire national security spectrum from peace to war and tooth to tail.

## B.2 United States

**Thomas Rona [Lib]:**

The strategic, operation, and tactical level competitions across the spectrum of peace, crisis, crisis escalation, conflict, war, war termination, and reconstitution/restoration, waged between competitors, adversaries or enemies using information means to achieve their objectives.

**Emmer Paige 1995; ook definitie van het (US) DoD:**

Actions taken to achieve information superiority in support of national military strategy by affecting adversary information and information systems while leveraging and defending our information and systems.

**US AIR FORCE:**

Any action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting ourselves against those actions; and exploiting our own military information functions.

**US ARMY (DoD definitie van IW):**

Actions taken to achieve information superiority by affecting adversary information, information based processes, and information systems, while defending ones own information, information based processes, and information systems.

**US Joint Chiefs of Staff [CJCSI 3210.01, 1996] definitie van IW:**

Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks **while defending** one's own information, information-based processes, information systems, and computer-based networks.

(een eerste versie van deze definitie uit 1994, opgesteld door het Defense Science Board, voegde daar in de eerste zin aan toe "in support of military strategy".

**US Joint Chiefs of Staff over Command and Control Warfare (C2W):**

The integrated use of operations security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare (EW), and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary command and control capabilities while protecting friendly C2 capabilities against such actions. Command and control warfare applies across the operational continuum and all levels of conflict.
Also called C2W. C2W applies across the operational continuum and all levels of conflict. C2W is both offensive and defensive:

**Counter-C2.** To prevent effective C2 of adversary forces by denying information to, influencing, degrading or destroying the adversary C2 system.

**C2-protection.** To maintain effective command and control of own forces by turning to friendly advantage or negating adversary efforts to deny information to, influence, degrade or destroy the friendly C2 system.

**US DoD over Command and Control Warfare (C2W):**

C2W is the military strategy that implements Information Warfare on the battlefield and integrates physical destruction. Its objective is to decapitate the enemy's command structure from its body of command forces.

**US DoD over Information Superiority (part of Information Operations):**

**Information Superiority** is the capability to collect, process and disseminate an uninterrupted flow of information, while exploiting or denying an adversary's ability to do the same [JV2010] (ook: DoDD S-3600.1).
(*kwantitatief aspect*)

**US DoD over Information Dominance (ID):**

**Information Dominance** is the degree of *information superiority* that allows the possessor to use information systems and capabilities to achieve an operational advantage in a conflict or to control the situations short of war, while denying those capabilities to the adversary [FM 100-6 definition].
(*kwalitatief aspect*)

(ID is a condition that results from the use of offensive and defensive Info Ops to build a comprehensive knowledge advantage at a time, place and on decision issues critical to accomplish the mission quickly and decisively. Steps: Shape the infospace, Provide C2 protection, Conduct C2 attack,, Practice spectrum adaptability, Establish situation understanding, Achieve high performance)

**US DoD over Information Operations (Info Ops):**

**Information Operations** are: Continuous *military* operations within the *military* information environment that enable, enhance, and protect the friendly force's ability to collect, process, and act on information to achieve an advantage across the full range of military operations. Info Ops include the interacting with the global information environment and exploiting or denying an adversary's information and decision capabilities. [FM 100-6 definition].
(*kwalitatief aspect*)

**US Special Operations Command (SOCOM) over Info Ops:**

**Information Operations** is a *strategy* that integrates various capabilities to gain *information superiority* that supports national and/or military objective(s).
(not just a weapon, means or capability) [InfoW98]

**US Joint Chiefs of Staff Joint Pub 3-13 about Info Ops:**

**Information Operations** capitalize on the growning sophistication, connectivity, and reliance on informatio technology. Info Ops target information technology or information systems in order to affect the information-based process whether human or automated.
(Info Ops battlespace is the infrastructure) [JP3-13]

## B.3 United Kingdom

**UK Royal Navy (Captain Patrick Tyrell):** [25]

The deliberate, unauthorised and systematic attack on critical national information activities to exploit the information contained within the system, deny service to the authorised user, modify or corrupt data.

## B.4 Duitsland

**Duitse Defensie (1997) concept IW-definitie door het Bundeswehr-kantoor voor studies en oefeningen, werkgroep Force2020 [HSAIW]:**

"Information Warfare comprises all arrangements and measures which enable a nation or supranational organization, especially if a crises develops, a conflict escalates or a threat emerges, to ensure the political, economic or military freedom of decision-making and freedom of action both by the interference with, manipulation or elimination of enemy information, information-based processes and information infrastructures and by defense of such attacks on basis of an information advantage.
Information Warfare uses the results of available procedures of information processing, adds new forms and relies on an efficient information management."

## B.5 China

**China's IW-opvatting [Sig0798]:**

"Information Warfare is gradually changing from preserving oneself and wiping out the enemy to preserving oneself and controlling the opponent. Information Warfare includes EW, *tactical deception*, *strategic deterrence*, *propaganda warfare*, PSYOPS, NetWar and *structural sabotage*, all of which have something to do with strategy."

---

25 Pat Tyrrell was van 1992 tot 1996 Assistant Director CIS en is sinds 4/97 Commander van het Defense Intelligence and Security School at Chicksands. Hij maakt deel uit van de Kemble Group, een 'denktank' op het gebied van management issues die voortvloeien uit de informatiemaatschappij ontwikkelingen.

# REPORT DOCUMENTATION PAGE
## (MOD-NL)

| 1. DEFENCE REPORT NO (MOD-NL) | 2. RECIPIENT'S ACCESSION NO | 3. PERFORMING ORGANIZATION REPORT NO |
|---|---|---|
| TD99-0228 | | FEL-99-A142 |
| **4. PROJECT/TASK/WORK UNIT NO** | **5. CONTRACT NO** | **6. REPORT DATE** |
| 28853 | A99D603 | July 1999 |
| **7. NUMBER OF PAGES** | **8. NUMBER OF REFERENCES** | **9. TYPE OF REPORT AND DATES COVERED** |
| 90 (incl appendices, excl RDP & distribution list) | 56 | Final |

**10. TITLE AND SUBTITLE**

Verkenning naar Information Warfare, Information Operations en Information Assurance
(Survey of Information Warfare, Information Operations and Information Assurance)

**11. AUTHOR(S)**

H.A.M. Luiijf

**12. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**

TNO Physics and Electronics Laboratory, PO Box 96864, 2509 JG The Hague, The Netherlands
Oude Waalsdorperweg 63, The Hague, The Netherlands

**13. SPONSORING AGENCY NAME(S) AND ADDRESS(ES)**

Defensiestaf/Conceptuele Zaken
Plein 4, 2511 CR The Hague, The Netherlands

**14. SUPPLEMENTARY NOTES**

The classification designation Ongerubriceerd is equivalent to Unclassified, Stg. Confidentieel is equivalent to Confidential and Stg. Geheim is equivalent to Secret.

**15. ABSTRACT (MAXIMUM 200 WORDS (1044 BYTE))**

Research survey on the phenomena Information Warfare, Information Operations (Info Ops) and Information Assurance. History, development, definitions and developments in various countries around the globe. Appendix with list of abbreviations of terms in these fields.

| 16. DESCRIPTORS | IDENTIFIERS |
|---|---|
| Information Warfare<br>Information Security | Information Operations<br>Information Assurance<br>Critical Infrastructure Protection |

| 17a. SECURITY CLASSIFICATION (OF REPORT) | 17b. SECURITY CLASSIFICATION (OF PAGE) | 17c. SECURITY CLASSIFICATION (OF ABSTRACT) |
|---|---|---|
| Ongerubriceerd | Ongerubriceerd | Ongerubriceerd |

| 18. DISTRIBUTION AVAILABILITY STATEMENT | 17d. SECURITY CLASSIFICATION (OF TITLES) |
|---|---|
| Unlimited | Ongerubriceerd |

# Distributielijst

1. DWOO
2. HWO-KM
3. HWO-KL
4. HWO-KLu
5. HWO-CO
6. MinDef/DS/Defensiestaf/Conceptuele Zaken, t.a.v. Kol. H. Sonneveld
7. MinDef/DS/Defensiestaf/Conceptuele Zaken, t.a.v. LKol. J.J.M.G. Maenen
8. DM&P TNO-DO
9. DM&P TNO-DO, t.a.v. Ir. W.C. Borawitz
10. Directeur TNO-TM
11. Accountcoördinator KL
12. Accountcoördinator CO

13 t/m 15. Bibliotheek KMA

16. KMA, t.a.v. BGen. Prof. J.M.J. Bosch
17. KMA, t.a.v. Lkol. Ing. A. Mollema
18. KL/LAS/BO/OB, t.a.v. Lkol. A. Dondorp
19. KL/LAS/BO/OB, t.a.v. Lkol. G.J. Kanis
20. DM/KM/WO, t.a.v. LTZ1. A.W. Velema
21. KM/MARSTAF, t.a.v. KTZ. J. Buzepol
22. KM/MARSTAF/PHCIS, t.a.v. KLTZ. Q.P.F. Buizert
23. OC-Ede/KC/MID/HsiePL, t.a.v. Lkol. W.G.F. Kempen
24. OC-Ede/KC/MID/HsiePL, t.a.v. Maj. H.J. Mulder
25. MID/ACIV/BCI, t.a.v. Lkol. P.J. Post Uiterweer
26. MinDef/DGEF/DOI/BA, t.a.v. dhr. E.D. de Graaf
27. MinDef/DS/CIS, t.a.v. Kol. Ir. A.P. Coppens
28. MinBZK/DGOB/DIOS/Infrastructuur en Continuïteit, t.a.v. Mr. J.J. Moelker MPA
29. MinV&W/DGTP/Informatie-infrastructuren, t.a.v. dr. G.A.A.M. Broesterhuizen
30. Directie TNO-STB, t.a.v. Ir. L. Hoedenmaker
31. TNO-TM, t.a.v. Dr. H.J. Griffioen-Young
32. TNO-TM, t.a.v. Drs. R. van der Kleij
33. TNO-TM, t.a.v. Dr. P.J. Werkhoven
34. TNO-TM, bibliotheek
35. Directeur TNO-FEL
36. Adjunct-directeur TNO-FEL, daarna reserve
37. Archief TNO-FEL, in bruikleen aan MPC
38. Archief TNO-FEL, in bruikleen aan Accountmanager KM
39. Archief TNO-FEL, in bruikleen aan Accountmanager KL
40. Archief TNO-FEL, in bruikleen aan Accountmanager Klu
41. Archief TNO-FEL, in bruikleen aan Accountmanager CO
42. Archief TNO-FEL, in bruikleen aan Drs. Ing. C.W. D'Huij
43. Archief TNO-FEL, in bruikleen aan Drs. Ing. J. Dexel
44. Archief TNO-FEL, in bruikleen aan Drs. J.L. Joppe
45. Archief TNO-FEL, in bruikleen aan Dr. M.H.A. Klaver
46. Archief TNO-FEL, in bruikleen aan Drs. C.T.J. van Langen
47. Archief TNO-FEL, in bruikleen aan Ir. H.A.M. Luiijf
48. Archief TNO-FEL, in bruikleen aan Ir. A.P.T.M. Onderwater
49. Archief TNO-FEL, in bruikleen aan Ir. K.H.W. Pasman
50. Archief TNO-FEL, in bruikleen aan Ir. M.J. van de Scheur
51. Archief TNO-FEL, in bruikleen aan Dr. L. Smit
52. Archief TNO-FEL, in bruikleen aan Ir. P. van de Schulein
53. Archief TNO-FEL, in bruikleen aan Ing. P.J.A. Verhaar
54. Archief TNO-FEL, in bruikleen aan Ir. R.F.W.M. Willems
55. Archief TNO-FEL, in bruikleen aan Prof. Dr. Ir. A.P.M. Zwamborn
56. Documentatie TNO-FEL
57. Reserve

Indien binnen de krijgsmacht extra exemplaren van dit rapport worden gewenst door personen of instanties die niet op de verzendlijst voorkomen, dan dienen deze aangevraagd te worden bij het betreffende Hoofd Wetenschappelijk Onderzoek of, indien het een K-opdracht betreft, bij de Directeur Wetenschappelijk Onderzoek en Ontwikkeling.

*) Beperkt rapport (titelblad, managementuittreksel, RDP en distributielijst).